NNTDM 17 (2011), 2, 4-11

Note on the matrix Fermat's equation [1]

Aleksander Grytczuk and Izabela Kurzydło

Faculty of Mathematics, Computer Science and Econometrics,
University of Zielona Góra,
65-516 Zielona Góra, Poland
emails: $\{A.Grytczuk, I.Kurzydlo\}@wmie.uz.zgora.pl$

Abstract. We consider the Fermat's equation

$$X^n + Y^n = Z^n \tag{F}$$

in the set of 2×2 rational matrices. We give some necessary condition of solvabillity of this equation.

Keywords. The matrix equation, the matrix Fermat's equation, powers of matrices

AMS classification. 15A24,15A42

1 Introduction

The Fermat's equation (F) in $M_2(\mathbb{Q})$ was considered by Barnett and Weitkamp in 1961 what was described by P. Ribenboim in monograph [13]. In 1966 R. Z. Domiaty [4] discovered that the equation (F) has infinitely many solutions in $M_2(\mathbb{Z})$ for $n = 4$. The solvability of (F) in $\mathrm{GL}_2(\mathbb{Z})$ was first investigated by L. N. Vaserstein [14]. A. Khazanov in [9] gave necessary and sufficient conditions for solvability (F) for X, Y, Z belonging to $SL_2(\mathbb{Z})$,-$SL_3(\mathbb{Z})$, $GL_3(\mathbb{Z})$. A. Gryczuk [7] proved some necessary condition to satisfy (F) in integral 2×2 matrices X, Y, Z, and in [5] he gave an extension of this result. Studies connected with Khazanov's results effected too H. Qin [12]. The equation of Fermat was investigated by Z. Patay and A. Szakas ([11]}, Z. Cao and A. Grytczuk ([2]). In [3] Z. Cao and A. Grytczuk gave a necessary and sufficient condition for solvability (F) for $X, Y, Z \in \overline{SL_2(\mathbb{Z})}$.

For $X = A^x, Y = A^y, Z = A^z$ we obtain from (F) the following equation

$$A^{nx} + A^{ny} = A^{nz}. \tag{1}$$

The necessary and sufficient conditions for solvabitity of the equation (1) in natural number x, y, z and $n > 2$, where $A \in M_2(\mathbb{Z})$ were given by Le and Li in [10]. Another proof of this result was gaven by A. Grytczuk ([6]). In the paper [8] we considered the extension of the equation (1)

[1] This paper is partly supported by EFS (European Social Funds).

$$A^{mx} + A^{my} + A^{mz} = A^{mw}, \tag{2}$$

where $A \in M_2(\mathbb{Z})$.We gave ([8]) the necessary and sufficient conditions for solvabitity of the equation (2) in natural number x, y, z, w and $n > 2$.

In this paper we give the following necessary condition for solvabillity of the Fermat's equation (F) in the set of 2×2 rational matrices $M_2(\mathbb{Q})$:

Theorem 1 *Let* $X, Y, Z \in M_2(\mathbb{Q})$.

Let $\det X = \det Y = k_1, \det Z = k_2,$*where* $k_1 \neq k_2,\ k_1, k_2 \neq 0,$ *and*

$$Z^{-1}X = XZ^{-1}, Z^{-1}Y = YZ^{-1},$$

$$TrZ^{-1}X, TrZ^{-1}Y \in \{0, 2\}.$$

If the Fermat's equation

$$X^n + Y^n = Z^n \tag{F}$$

has a solution, then $n = 2$ *with*

$$\frac{k_1}{k_2} = -\frac{1}{2}.$$

In the proof of Theorem 1 we use the following lemma which can easy prove by induction:

Lemma 1 *If* $A \in M_2(\mathbb{Q}),\ A = \begin{pmatrix} \frac{a}{b} & \frac{c}{d} \\ \frac{e}{f} & \frac{g}{h} \end{pmatrix}$, $b,\ d,\ f,\ h \neq 0,$ *then*

$$A^n = \begin{pmatrix} F\left(\frac{a}{b}\right) & \frac{c}{d}w \\ \frac{e}{f}w & F\left(\frac{g}{h}\right) \end{pmatrix},\ n \geqslant 2,$$

where w *is a rational number,* $F\left(\frac{a}{b}\right),\ F\left(\frac{g}{h}\right)$ *are polynomials of degree* n,

$$F\left(\frac{a}{b}\right) - F\left(\frac{g}{h}\right) = \left(\frac{a}{b} - \frac{e}{f}\right) w.$$

Lemma 1 for $A \in M_2(\mathbb{Z})$ was proved in by K. Białek and A. Grytczuk in [1].

2 The proof of Theorem 1.

Let the assumptions of the Theorem 1 be satisfied.

From the equation (F) we obtain

$$\left(Z^{-1}X\right)^n + \left(Z^{-1}Y\right)^n = I. \tag{3}$$

Denote

$$A = Z^{-1}X = XZ^{-1}, B = Z^{-1}Y = YZ^{-1}.$$

Hence, from (3) we have

$$A^n + B^n = I. \tag{4}$$

Let

$$A = \begin{pmatrix} \frac{a_1}{b_1} & \frac{c_1}{d_1} \\ \frac{e_1}{f_1} & \frac{g_1}{h_1} \end{pmatrix}, B = \begin{pmatrix} \frac{a_2}{b_2} & \frac{c_2}{d_2} \\ \frac{e_2}{f_2} & \frac{g_2}{h_2} \end{pmatrix}.$$

From Lemma 1 we obtain

$$A^n = \begin{pmatrix} F_1\left(\frac{a_1}{b_1}\right) & \frac{c_1}{d_1}w_1 \\ \frac{e_1}{f_1}w_1 & F_1\left(\frac{g_1}{h_1}\right) \end{pmatrix}, \qquad B^n = \begin{pmatrix} F_2\left(\frac{a_2}{b_2}\right) & \frac{c_2}{d_2}w_2 \\ \frac{e_2}{f_2}w_2 & F_2\left(\frac{g_2}{h_2}\right) \end{pmatrix}, \tag{5}$$

where w_1, w_2 are rational numbers,

$$\begin{aligned} F_1\left(\frac{a_1}{b_1}\right) - F_1\left(\frac{g_1}{h_1}\right) &= \left(\frac{a_1}{b_1} - \frac{e_1}{f_1}\right) w_1, \\ F_2\left(\frac{a_2}{b_2}\right) - F_2\left(\frac{g_2}{h_2}\right) &= \left(\frac{a_2}{b_2} - \frac{e_2}{f_2}\right) w_2 \end{aligned}$$

By (4) and (5) it follows that

$$\begin{pmatrix} F_1\left(\frac{a_1}{b_1}\right) & \frac{c_1}{d_1}w_1 \\ \frac{e_1}{f_1}w_1 & F_1\left(\frac{g_1}{h_1}\right) \end{pmatrix} + \begin{pmatrix} F_2\left(\frac{a_2}{b_2}\right) & \frac{c_2}{d_2}w_2 \\ \frac{e_2}{f_2}w_2 & F_2\left(\frac{g_2}{h_2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{6}$$

From (6) we give

$$\begin{aligned} &F_1\left(\frac{a_1}{b_1}\right) + F_2\left(\frac{a_2}{b_2}\right) = 1 \\ &F_1\left(\frac{g_1}{h_1}\right) + F_2\left(\frac{g_2}{h_2}\right) = 1 \\ &\frac{c_1}{d_1}w_1 + \frac{c_2}{d_2}w_2 = \frac{e_1}{f_1}w_1 + \frac{e_2}{f_2}w_2 = 0. \end{aligned} \tag{7}$$

From the known theorem of Cauchy we have

$$\det A^n = \det B^n = \left(\frac{k_1}{k_2}\right)^n. \tag{8}$$

From the other hand from (5) we obtain

$$\begin{aligned} \det A^n &= F_1\left(\frac{a_1}{b_1}\right) F_1\left(\frac{g_1}{h_1}\right) - \frac{c_1 e_1}{d_1 f_1} w_1^2, \\ \det B^n &= F_2\left(\frac{a_2}{b_2}\right) F_2\left(\frac{g_2}{h_2}\right) - \frac{c_2 e_2}{d_2 f_2} w_2^2. \end{aligned} \tag{9}$$

By (8), (9) and the last equation in (7) it follows that

$$F_1\left(\frac{a_1}{b_1}\right)F_1\left(\frac{g_1}{h_1}\right)=F_2\left(\frac{a_2}{b_2}\right)F_2\left(\frac{g_2}{h_2}\right). \tag{10}$$

From (5) we have

$$TrA^n=F_1\left(\frac{a_1}{b_1}\right)+F_1\left(\frac{g_1}{h_1}\right), \tag{11}$$

$$TrB^n=F_2\left(\frac{a_2}{b_2}\right)+F_2\left(\frac{g_2}{h_2}\right). \tag{12}$$

From (7) we give

$$F_2\left(\frac{g_2}{h_2}\right)=1-F_1\left(\frac{g_1}{h_1}\right), \tag{13}$$

$$F_2\left(\frac{a_2}{b_2}\right)=1-F_1\left(\frac{a_1}{b_1}\right). \tag{14}$$

From (10) and (13) we obtain

$$\left(F_1\left(\frac{a_1}{b_1}\right)+F_2\left(\frac{a_2}{b_2}\right)\right)F_1\left(\frac{g_1}{h_1}\right)=F_2\left(\frac{a_2}{b_2}\right) \tag{15}$$

By (15) and (7) it follows that

$$F_1\left(\frac{g_1}{h_1}\right)=F_2\left(\frac{a_2}{b_2}\right) \tag{16}$$

Similary we can prove that

$$F_1\left(\frac{a_1}{b_1}\right)=F_2\left(\frac{g_2}{h_2}\right) \tag{17}$$

Therefore from (7), (16), (17), (11) and (12) we obtain

$$\begin{aligned} TrA^n&=F_1\left(\frac{a_1}{b_1}\right)+F_2\left(\frac{a_2}{b_2}\right)=1,\\ TrB^n&=F_1\left(\frac{g_1}{h_1}\right)+F_2\left(\frac{g_2}{h_2}\right)=1. \end{aligned} \tag{18}$$

Let λ_1, λ_2 be the eigenvalues of the matrix A. Then λ_1^n, λ_2^n are the eigenvalues of the matrix A^n.

From (18) and (8) we give

$$TrA^n=\lambda_1^n+\lambda_2^n=1, \tag{19}$$

$$\det A^n=\lambda_1^n\lambda_2^n=\left(\frac{k_1}{k_2}\right)^n. \tag{20}$$

Let $f(\lambda)=\lambda^2-(TrA)\lambda+\det A$ be the characteristic polynomial of the matrix A.

Then

$$\lambda_1 = \frac{TrA + \sqrt{(TrA)^2 - 4\det A}}{2},$$
$$\lambda_2 = \frac{TrA - \sqrt{(TrA)^2 - 4\det A}}{2}. \tag{21}$$

are the characteristic roots of A.

We consider the following cases:
1^0 $TrA = 0$

Then from (21) we obtain

$$\lambda_1 = \sqrt{-\frac{k_1}{k_2}}, \qquad \lambda_2 = -\sqrt{-\frac{k_1}{k_2}}. \tag{22}$$

For $n = 2k+1$ from (22) we obtain

$$TrA^n = 0$$

what is contrary with (19).

For $n = 2k$ from (19) and (22) we obtain

$$TrA^n = 2\left(\sqrt{-\frac{k_1}{k_2}}\right)^n = 1,$$

thus

$$\left(\sqrt{-\frac{k_1}{k_2}}\right)^n = \frac{1}{2} \tag{23}$$

what is contrary for $k_1, k_2 > 0$ or $k_1, k_2 < 0$.

If $k_1 < 0$ and $k_2 > 0$ or $k_2 < 0$ and $k_1 > 0$, then

$$-\frac{k_1}{k_2} > 0.$$

Then the equation (23) is true for $n = 2$ and $\frac{k_1}{k_2} = -\frac{1}{2}$.

For $n = 2k$, where $k_1 < 0$ and $k_2 > 0$ or $k_2 < 0$ and $k_1 > 0$ from (22) we have

$$\det A^n = (-1)^n \left(\frac{k_1}{k_2}\right)^n = \left(\frac{k_1}{k_2}\right)^n.$$

Therefore (20) and (19) are satisfied for $n = 2$ with $\frac{k_1}{k_2} = -\frac{1}{2}$.

2^0 $TrA = 2$

Then from (21) we get

$$\lambda_1 = 1 + \sqrt{1 - \frac{k_1}{k_2}}, \qquad \lambda_2 = 1 - \sqrt{1 - \frac{k_1}{k_2}}.$$

We have

$$TrA^n = \left(1 + \sqrt{1 - \frac{k_1}{k_2}}\right)^n + \left(1 - \sqrt{1 - \frac{k_1}{k_2}}\right)^n$$

$$= 2 + 2\tbinom{n}{2}\left(\sqrt{1 - \frac{k_1}{k_2}}\right)^2 + 2\tbinom{n}{4}\left(\sqrt{1 - \frac{k_1}{k_2}}\right)^4 + 2\tbinom{n}{6}\left(1 - \frac{k_1}{k_2}\right)^6 + ..+$$

$$+ \left(\sqrt{1 - \frac{k_1}{k_2}}\right)^n + \left(-\sqrt{1 - \frac{k_1}{k_2}}\right)^n \tag{24}$$

$$= 2 + 2\tbinom{n}{2}\left(1 - \frac{k_1}{k_2}\right) + 2\tbinom{n}{4}\left(1 - \frac{k_1}{k_2}\right)^2 + 2\tbinom{n}{6}\left(1 - \frac{k_1}{k_2}\right)^3 + ...+$$

$$+ \left(\sqrt{1 - \frac{k_1}{k_2}}\right)^n + \left(-\sqrt{1 - \frac{k_1}{k_2}}\right)^n.$$

Let $n = 2k$.
Then we have

$$\left(\sqrt{1 - \frac{k_1}{k_2}}\right)^n + \left(-\sqrt{1 - \frac{k_1}{k_2}}\right)^n = 2\left(1 - \frac{k_1}{k_2}\right). \tag{25}$$

From (24), (25) and (19) we obtain

$$1 + \binom{n}{2}\left(1 - \frac{k_1}{k_2}\right) + ... + \binom{n}{n-2}\left(1 - \frac{k_1}{k_2}\right)^{\frac{1}{2}(n-2)} + \left(1 - \frac{k_1}{k_2}\right)^k = \frac{1}{2}. \tag{26}$$

Assume that $\frac{k_1}{k_2} < 1$.
Then

$$1 + \binom{n}{2}\left(1 - \frac{k_1}{k_2}\right) + ... + \binom{n}{n-2}\left(1 - \frac{k_1}{k_2}\right)^{\frac{1}{2}(n-2)} + \left(1 - \frac{k_1}{k_2}\right)^k > 1 > \frac{1}{2},$$

therefore the equation (26) does not hold.

Assume that $\frac{k_1}{k_2} > 1$.
Then we remark that (26) is not satisfied.

Let $n = 2k + 1$.

Then

$$\left(\sqrt{1-\frac{k_1}{k_2}}\right)^n + \left(-\sqrt{1-\frac{k_1}{k_2}}\right)^n = 0. \qquad (27)$$

From (24), (27) and (19) we have

$$1+\binom{n}{2}\left(1-\frac{k_1}{k_2}\right)+\binom{n}{4}\left(1-\frac{k_1}{k_2}\right)^2+...+\binom{n}{2k}\left(1-\frac{k_1}{k_2}\right)^k=\frac{1}{2}. \qquad (28)$$

If $0<\frac{k_1}{k_2}<1$,then

$$1+\binom{n}{2}\left(1-\frac{k_1}{k_2}\right)+\binom{n}{4}\left(1-\frac{k_1}{k_2}\right)^2+...+\binom{n}{2k}\left(1-\frac{k_1}{k_2}\right)^k>1>\frac{1}{2}$$

and the equation (28) is not satisfied.

If $\frac{k_1}{k_2}>1$,then

$$1+\binom{n}{2}\left(1-\frac{k_1}{k_2}\right)+\binom{n}{4}\left(1-\frac{k_1}{k_2}\right)^2+...+\binom{n}{2k}\left(1-\frac{k_1}{k_2}\right)^k\neq\frac{1}{2}.$$

Similary as for the matrix A we obtain for the matrix B and the proof of Theorem 1 is finished. ■

Example 1 *Let* $X=Y=\begin{pmatrix} 0 & 1 \\ \frac{1}{2} & 0 \end{pmatrix}$, $Z=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Then

$$\begin{aligned} Z^{-1} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \det X = \det Y = -\frac{1}{2}, \ \det Z = 1, \\ Z^{-1}X &= XZ^{-1}, Z^{-1}Y = YZ^{-1}, \\ \det A &= \det XZ^{-1} = -\frac{1}{2}, \quad TrA = 0. \end{aligned}$$

We have $X^2+Y^2=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=Z^2$.

References

[1] Białek,K. and Grytczuk, A., 1987, The equation of Fermat in $G_2(k)$ and $\mathbb{Q}(\sqrt{k})$, Acta Academiae Paedagogicae Agriensis. Matematika,**18**/11, 81-90.

[2] Cao, Z. and Grytczuk, A., 1998, Fermat's type equations in the set of $2x2$ integral matrices, Tsukuba J. Math., **22**, 637-643.

[3] Cao, Z. and Grytczuk, A., 2000, Some remarks on Fermat's equation in the set of matrices, Acta Acad. Paed. Agriensis, Sectio Math., **27**, 39-46.

[4] Domiaty, R. Z., 1966, Solutions of $x^4 + y^4 = z^4$ in $2x2$ integral matrices, Amer. Math. Monthly, **73**, 631.

[5] Grytczuk, A., 1997, Fermat's equation in the set of matrices and special functions, Studia Univ. Babes-Bolyai, Mathematica, **4**, 49-55.

[6] Grytczuk, A., 1998, On a conjecture about the equation $A^{mx} + A^{my} = A^{mz}$, Acta Acad. Paed. Agrieusis, Sectio Math., **25**, 61-70.

[7] Grytczuk, A., 1995, On Fermat's equation in the set of integral $2x2$ matrices, Period. Math. Hungar., **30**, 67-72.

[8] Grytczuk, A. and Kurzydło, I.,2009, The necessary and sufficient condition for the solvability of Diophantine matrix equation $A^{mx} + A^{my} + A^{mz} = A^{mw}$, Boletin de la Sociedad Matematica Mexicana.,**15**, 109-116.

[9] Khazanov, A., 1995, Fermat's equation in matrices, Serodica Math. J., **21**, 19-40.

[10] Le, M. and Li, C., 1995, On Fermat's equation in integral $2x2$ matrices, Period. Math. Hung., **31**, 219-222.

[11] Patay, Z. and Szakacs, A., 2002, On Fermat's problem in matrix rings and groups, Publ. Math. Debrecen, **61**/3-4, 487-494.

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

[13] Ribenboim, P., 1979, 13 Lectures on Fermat's Last Theorem (New York: Springer-Verlag).

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