TSUKUBA J. MATH.
Vol. 26 No. 2 (2002), 229–235

LJUNGGREN'S TRINOMIALS AND MATRIX EQUATION $A^x + A^y = A^z$

By

Aleksander GRYTCZUK and Jarosław GRYTCZUK

Abstract. We give some necessary and sufficient conditions for solvability of the matrix equation (*) $A^x + A^y = A^z$, with certain restrictions on integers x, y, z and a matrix $A \in M_k(\boldsymbol{Z})$, by applying Ljunggen's result on trinomials. Moreover, we obtain full solution of (*) for the case $k = 2$ by another technique.

1. Introduction

We consider the general problem of finding necessary and sufficient conditions for the matrix $A \in M_k(\boldsymbol{Z})$ to satisfy the equation

$$A^x + A^y = A^z \tag{$*$}$$

for some positive integers x, y and z. Le and Li [7] proved that if $A \in M_2(\boldsymbol{Z})$, then, for $x = mr,\ y = ms,\ z = mt$, where $m > 2$ and r, s, t are positive integers, (*) has a solution if and only if the matrix A is nilpotent or $\det A = TrA = 1$. Another proof of this result has been given in [5]. The restriction to multiplies of m is motivated by another matrix equation of the famous form, namely by the equation of Fermat

$$X^m + Y^m = Z^m. \tag{$**$}$$

In fact (*) is equivalent to Fermat's equation (**) for $X = A^r,\ Y = A^s$ and $Z = A^t$. We note, that if $m = 4$ the Domiaty [2] remarked that the equation (**) has infinitely many solutions in $M_2(\boldsymbol{Z})$ generated by Pythagorean triples. This fact is in opposition to the well-known case of ordinary integers, as proved by Wiles [13].

1999 Mathematics Subject Classification. Primary 11C20; Secondary 11D41.
Key words and phrases. Matrix equations, Ljunggren's trinomials.
Received May 16, 2000.
Revised April 15, 2002.

In this connection it is a very important problem to find a sufficient and necessary condition for solvability of Fermat's equation (**) in the set of matrices (cf. [10], [12]). Khazanov [6] found such conditions for the matrices $X, Y, Z \in SL_2(\boldsymbol{Z})$ and $X, Y, Z \in GL_3(\boldsymbol{Z})$. Further investigations connected with Khazanov's results have been given in the papers [1], [5], [7] and [9]. Some necessary condition for solvability of (**) in the set $M_2(\boldsymbol{Z})$ is contained in the paper [3]. In general case, it was proved in [4] that if the matrix $A \in M_k(\boldsymbol{C})$, $k \geq 2$ has at least one real eigenvalue $\alpha > \sqrt{2}$ and (*) is satisfied in positive integers x, y and z, then $\max\{x - z, y - z\} = -1$.

In the present paper we give an application of Ljunggren's [8] result on trinomials to find a sufficient and necessary condition for solvability of (*) in positive integers x, y and z under some restrictions for $A \in M_k(\boldsymbol{Z})$, $k \geq 2$ concerning the set of exponents x, y and z. Moreover, we present full solution of (*) for the case $k = 2$ without using Ljunggren's result on trinomials. In the first part of this paper we prove the following theorem.

Theorem 1. *Let $A \in M_k(\boldsymbol{Z})$, $k \geq 2$ be a given non-zero and non-singular matrix with the characteristic polynomial $f(t) = \det(tI - A) = t^k + a_1 t^{k-1} + \cdots + a_k$. Then the matrix equation (*) has a solution in positive integers x, y and z such that $x = y$ or $x = z$ or $y = z$ if and only if*

(i)

$$A^m = 2I,$$

where $m = k/\alpha$, $1 \leq \alpha \leq k$ is a divisor of k, $\det A = \pm 2^\alpha$ and $\alpha(z - x) = k \geq 2$. Moreover, if the positive integers x, y, z satisfy the conditions: $x > y > z$ and $x - z \geq 2(y - z) \geq k \geq 2$, with $(x - z, y - z) = (n, m) = d$ and $3 \nmid (x - z)/d + (y - z)/d$, then (*) has a solution, if and only if

(ii) *$a_i = 0$, for $i \neq m, k$, and $a_m = \varepsilon_1$ and $a_k = \det A = \varepsilon_2$, where $\varepsilon_1 = \pm 1$ and $\varepsilon_2 = \pm 1$ or if $3 \mid (x - z)/d + (y - z)/d$ then*

(iii)

$$A^{2d} + \varepsilon_1^{y-z} \varepsilon_2^{x-z} A^d + I = O \quad or \quad h(A) = O,$$

where $h(t)$ is irreducible factor of the polynomial $g(t)$ given by the equality

$$g(t) = t^{x-z} + \varepsilon_1 t^{y-z} + \varepsilon_2 = (t^{2d} + \varepsilon_1^{y-z} \varepsilon_2^{x-z} t^d + 1) h(t),$$

where $(x - z)/d, (y - z)/d$ are both odd and $\varepsilon_1 = 1$ or $(x - z)/d$ is even and $\varepsilon_2 = 1$ or $(y - z)/d$ is even and $\varepsilon_1 = \varepsilon_2$.

2. Basic Lemmas

In the proof of the Theorem 1 we use of the following Lemmas.

Lemma 1 ([11], p. 210). *Let A be a $k \times k$, $k \geq 2$ matrix with entries in the field K. Then each polynomial $g \in K[x]$ with property $g(A) = O$ is divisible by the minimal polynomial $m \in K[x]$ of the matrix A. In particular, the minimal polynomial m divides the characteristic polynomial $f \in K[x]$ of the matrix A and the polynomial f has the same roots, but possibly with different multiplicities.*

Remark 1. *The minimal polynomial of the matrix A is the unique polynomial $m \in K[x]$ of minimal degree with leading coefficient equal to one and such that $m(A) = O$.*

Lemma 2 (Ljunggren [8], Thm. 3, p. 69). *If $n = dn_1$, $m = dm_1$, $n \geq 2m$ where $(n_1, m_1) = 1$, then the polynomial $g(x) = x^n + \varepsilon_1 x^m + \varepsilon_2$, where $\varepsilon_1, \varepsilon_2 = \pm 1$ is irreducible, apart from the following three cases, when $n_1 + m_1 \equiv 0 \pmod 3$: 1^0 n_1, m_1 both odd and $\varepsilon_1 = 1$, 2^0 n_1 even and $\varepsilon_2 = 1$, 3^0 m_1 even and $\varepsilon_1 = \varepsilon_2$ and then $g(x) = (x^{2d} + \varepsilon_1^m \varepsilon_2^n x^d + 1)h(x)$, where $h(x)$ is an irreducible polynomial.*

3. Proof of the Theorem 1

Suppose that (*) has a solution in positive integers x, y and z and let the matrix $A \in M_k(\boldsymbol{Z})$ be a non-zero and non-singular matrix. First, we note that if $x = z$ or $y = z$ then (*) is impossible, since (*) reduces in these cases to the form $A^y = O$ or $A^x = O$. Both these equations imply $\det A = 0$, which contradicts the assumptions. If $x = y$ then (*) has the form

$$2A^x = A^z. \tag{3.1}$$

By (3.1) it follows that $x \neq z$ and $z > x$ and consequently we have

$$A^{z-x} = 2I. \tag{3.2}$$

From (3.2) we obtain $\det A^{z-x} = (\det A)^{z-x} = 2^k$, so $\det A = \pm 2^\alpha$, where $1 \leq \alpha \leq k$. Hence, $(\pm 2)^{\alpha(z-x)} = 2^k$ and $\alpha(z - x) = k \geq 2$, where α or $z - x$ is even if $\det A = -2^\alpha$ and $z - x = k/\alpha = m$. Then by (3.2) it follows that $A^m = 2I$ and the proof of (i) is finished. Now, we can consider the case when $x \neq y \neq z$. In this case, by the equation (*) and the assumptions about x, y and z it follows to consider the following equation:

$$A^{x-z} + A^{y-z} = I. \tag{3.3}$$

Let $d = (x - z, y - z) = (n, m)$ be the greatest common divisor of n and m and let $x - z \geq 2(y - z) \geq k \geq 2$ and denote by $g(t)$ the polynomial of the form

$$g(t) = t^{x-z} + t^{y-z} - 1. \tag{3.4}$$

Then by (3.3) it follows that $g(A) = O$. If $3 \nmid (x - z)/d + (y - z)/d$ then from Lemma 2 it follows that the polynomial $g(t)$ is irreducible and therefore the characteristic polynomial $f(t)$ of the matrix A is equal to $g(t)$ in (3.4). Comparing the coefficients and degrees of these polynomials we obtain the condition (ii). Let $3 \mid (x - z)/d + (y - z)/d$, then by Ljunggren's result given in Lemma 2 we obtain that

$$g(t) = (t^{2d} + \varepsilon_1^m \varepsilon_2^n t^d + 1)h(t). \tag{3.5}$$

From (3.5) in virtue of $g(A) = O$ we obtain that

$$A^{2d} + \varepsilon_1^m \varepsilon_2^n A^d + I = O \quad \text{or} \quad h(A) = O$$

with some restrictions concerning m, n, d and the polynomial $h(t)$ given by the assumptions of the Ljunggren's Lemma 2. The proof of the Theorem 1 is complete.

4. Full Solution of the Equation (*) for the Case $A \in M_2(\boldsymbol{Z})$

In this part of our paper we present full solution of the equation (*) in positive integers x, y and z in the case when the matrix A belongs to $M_2(\boldsymbol{Z})$. In this purpose we replace Ljunggren's result on trinomials by the following Lemma.

LEMMA 3 ([4]). *Let A be in $M_k(\boldsymbol{C})$, where $k \geq 2$ and $\boldsymbol{C}$ denotes the field of complex numbers. Suppose that A has at least one real eigenvalue $\alpha > \sqrt{2}$. If the equation (*) has a solution in positive integers x, y and z then* $\max\{x - z, y - z\} = -1$.

Now we prove the following theorem.

THEOREM 2. *Let $A \in M_2(\boldsymbol{Z})$ be a given non-zero matrix with* $\det A = s$ *and $Tr\ A = r$. Then the matrix equation* (*) *has a solution in positive integers x, y and z if and only if one of the following conditions holds*:

(i)

$$A = 2I,$$

(ii)

$$(r, s) = \{(0,0), (0,2), (0,-2), (1,1), (1,-1), (-1,-1)\}.$$

PROOF. Denote by $f(t) = \det(tI - A) = t^2 - (Tr\,A)t + \det A$ the characteristic polynomial of the matrix $A \in M_2(\boldsymbol{Z})$ and let $r = Tr\,A$ and $s = \det A$. Suppose that the matrix A is non-singular, so $s = \det A \neq 0$ and let positive integers x, y and z satisfy the equation (*). If $x = z$ or $y = z$ then (*) reduces to $A^y = O$ or $A^x = O$, which is impossible, because $s = \det A \neq 0$. If $x = y$ then (*) has the form: $2A^x = A^z$. We observe that if $x \geq z$ then we have $2A^{x-z} = I$, which implies $4 \det A^{x-z} = 4(\det A)^{x-z} = 1$ and we get a contradiction. Hence, $x < z$ and we obtain the following equation:

$$A^{z-x} = 2I. \tag{4.1}$$

From (4.1) it follows that $\det A^{z-x} = (\det A)^{z-x} = 4$ and consequently $\det A = \pm 2$ and $z - x = 2$ or $\det A = 4$ and $z - x = 1$. The case of $z - x = 1$ implies by (4.1) the condition (i) of the Theorem 2. In the case of $z - x = 2$ and $s = \det A = \pm 2$ by (4.1) it follows that

$$A^2 = 2I. \tag{4.2}$$

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a given matrix with entries $a, b, c, d \in \boldsymbol{Z}$. Then by (4.1) it follows that

$$A^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & d^2 + bc \end{pmatrix} = 2I = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}. \tag{4.3}$$

Analyzing the equation (4.3) we obtain that $b \neq 0$ and $c \neq 0$, so implies $a + d = r = 0$. From this fact in virtue of $s = \det A = \pm 2$ we obtain $(r, s) = (0, 2)$; $(0, -2)$.

Now, we can consider the case when $x \neq y \neq z$ and $s = \det A \neq 0, \pm 2$ and $A \neq 2I$. In these cases the equation (*) implies:

$$A^{x-z} + A^{y-z} = I, \quad \text{if } \min\{x, y, z\} = z \tag{4.4}$$

$$A^{x-y} + I = A^{z-y}, \quad \text{if } \min\{x, y, z\} = y \tag{4.5}$$

$$I + A^{y-x} = A^{z-x}, \quad \text{if } \min\{x, y, z\} = x. \tag{4.6}$$

For the corresponding equations (4.4)–(4.6) let $g(t)$ be associated polynomial of the form:

$$g(t) = t^{x-z} + t^{y-z} - 1, \quad \text{if (4.4) holds} \tag{P1}$$

$$g(t) = t^{x-y} - t^{z-y} + 1, \quad \text{if (4.5) holds} \tag{P2}$$

$$g(t) = t^{y-x} - t^{z-x} + 1, \quad \text{if (4.6) holds.} \tag{P3}$$

From (P1)–(P3) and (4.4)–(4.6) we obtain $g(A) = O$. Hence, by Lemma 1 it follows that if $m(t)$ is the minimal polynomial then we have $m(t) \mid g(t)$. In this connection we consider two cases: 1^0 $f(t) = t^2 - tr + s$ is an irreducible characteristic polynomial of the matrix A, 2^0 $f(t)$ is reducible polynomial. In the case 1^0 we have $f(t) = m(t)$ and therefore $f(t) \mid g(t)$, which by (P1)–(P3) implies

$$(4.7) \quad f(t) \mid t^{x-z} + t^{y-z} - 1, \text{ or } f(t) \mid t^{x-y} - t^{z-y} + 1, \text{ or } f(t) \mid t^{y-x} - t^{z-x} + 1.$$

From (4.7) in the case of $t = 0$ we get $f(0) \mid \pm 1$. Since $f(0) = s$, then $s = \pm 1$. On the other hand putting in (4.7) $t = 1$ we obtain $f(1) \mid \pm 1$. Since $f(1) = 1 - r + s$ and $s = \pm 1$ we get the following possibilities to consider:

$$(4.8) \qquad (r, s) = \{(1,1), (3,1), (-1,-1), (1,-1)\}.$$

Consider the case when $(r, s) = (3, 1)$. In this case the characteristic polynomial has the form: $f(t) = t^2 - 3t + 1$ and we have $\Delta = 5$ and the characteristic roots α, β of this polynomial are equal to $\alpha = (3 + \sqrt{5})/2$ and $\beta = (3 - \sqrt{5})/2$. Since $\alpha > \sqrt{2}$ then by Lemma 3 it follows that $\max\{x - z, y - z\} = -1$. Suppose that $\max\{x - z, y - z\} = x - z$. Then we have $x - z = -1$, so $z = x + 1$ and (*) implies

$$(4.9) \qquad A^x(A - I) = A^y.$$

Since $s = \det A = 1$ from (4.9) we obtain $\det(A - I) = 1$. If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then the condition $\det(A - I) = 1$ implies $(a - 1)(d - 1) - bc = 1$ and consequently $ad - bc - (a + d) = 0$. Since $ad - bc = s = 1$ and $a + d = Tr\, A = r$, thus we obtain $r = 1$, which is contrary to the fact that $r = 3$. Therefore, in the case of $(r, s) = (3, 1)$ the equation (*) has no solution. In a similar way we obtain a contradiction for the case if $\max\{x - z, y - z\} = y - z$.

It remains to consider the case 2^0 when the characteristic polynomial $f(t)$ is reducible. In this case we have $f(t) = (t - \alpha)(t - \beta)$, where $\alpha, \beta \in \boldsymbol{Z}$. From (*) and the assumption that A is non-singular matrix, it follows that $\det A = \pm 1$ and in virtue of $\det A = \alpha\beta$ we get $\alpha\beta = \pm 1$. Hence, $\alpha = \beta = 1$ or $\alpha = 1$ and $\beta = -1$ or $\alpha = -1$ and $\beta = 1$. For these cases we obtain that $A = I$ or $A = -I$ and the equation (*) has no solutions in positive integers $x \neq y \neq z$. Now, we can consider the final part of the proof. If the non-zero matrix $A \in M_2(\boldsymbol{Z})$ is singular, then $\det A = 0$. In this case, by simple inductive way, we get $A^m = (Tr\, A)^{m-1} A$ for all positive integers m. Using this formula and the assumption that $A \neq O$ we obtain that (*) reduces to the form:

$$(4.10) \qquad r^{x-1} + r^{y-1} = r^{z-1},$$

where $r = Tr\,A \in \boldsymbol{Z}$. It is easy to see that the equation (4.10) has a solution with positive integers $x \neq y \neq z$ and an integer r if and only if $r = 0$ or $r = 2$. Summarizing, we get that the condition (ii) is satisfied and the proof of the Theorem 2 is complete. ■

Acknowledgement 1

We would like to thank the referee for his suggestions and valuable remarks for the improvement of the exposition of this paper.

References

[1] Z. Cao and A. Grytczuk, Fermat's type equations in the set of 2×2 integral matrices, Tsukuba J. Math. **22** (1998), 637–643.
[2] R. Z. Domiaty, Solution of $x^4 + y^4 = z^4$ in 2×2 integral matrices, Amer. Math. Monthly, **73** (1966), 631.
[3] A. Grytczuk, On Fermat's equation in the set of integral 2×2 matrices, Period. Math. Hung. **30** (1995), 65–72.
[4] A. Grytczuk, Note on Fermat's type equation in the set of $n \times n$ matrices, Discuss. Math. **17** (1997), 19–23.
[5] A. Grytczuk, On a conjecture about the equation $A^{mx} + A^{my} = A^{mz}$, ActaAcad. Paed. Agriensis, Sectio Math. **25** (1998), 61–70.
[6] A. Khazanov, Fermat's equation in matrices, Serdica Math. J. **21** (1995), 19–40.
[7] M. Le and C. Li, On Fermat's equation in integral 2×2 matrices, Period. Math. Hung. **31** (1995), 219–222.
[8] W. Ljunggren, On the irreducibility of certain trinomials and quadrinomials, Math. Scand. **8** (1960), 65–70.
[9] H. Qin, Fermat's problem and Goldbach problem over $M_n Z$, Linear Algebra Appl. **236** (1996), 131–135.
[10] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer-Verlag. 1979.
[11] K. Spindler, Abstract Algebra with Applications, Marcel Dekker, New York, 1994.
[12] L. N. Vaserstein, Non-commutative Number Theory, Contemp. Math. **83** (1989), 445–449.
[13] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, Annals of Math., **141** (1995), 443–551.

Institute of Mathematics,
University of Zielona Góra.
Department of Algebra and Number Theory,
65-069 Zielona Góra, Poland
E-mail address: A.Grytczuk@im.uz.zgora.pl

Institute of Mathematics,
University of Zielona Góra,
65-246 Zielona Góra,
Poland
E-mail address: J.Grytczuk@im.uz.zgora.pl