On a conjecture about the equation

$$A^{mx} + A^{my} = A^{mz}$$

ALEKSANDER GRYTCZUK

Abstract. Let A be a given integral 2×2 matrix. We prove that the equation

$$A^{mx} + A^{my} = A^{mz}$$

has a solution in positive integers x,y,z and m>2 if and only if the matrix A is a nilpotent matrix or the matrix A has an eigenvalue $\alpha = \frac{1+i\sqrt{3}}{2}$.

1. Introduction

First we note that (\star) is equivalent to the following Fermat's equation

$$(1) X^m + Y^m = Z^m, \quad m > 2,$$

where $X = A^x$, $Y = A^y$ and $Z = A^z$.

It has been recently proved by A. WILES [12], R. TAYLOR and A. WILES [11] that (1) has no solution in nonzero integers X, Y, Z if m > 2. But, in contrast to the classical case, the Fermat's equation (1) has infinitely many solutions in 2×2 integral matrices X, Y, Z for m = 4. This fact was discovered by R. Z. DOMIATY [2] in 1966. Namely, he proved that, if

$$X = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} \text{ and } Z = \begin{pmatrix} 0 & 1 \\ c & 0 \end{pmatrix},$$

where a, b, c are integer solutions of the Pythagorean equation $a^2 + b^2 = c^2$, then

$$X^4 + Y^4 = Z^4.$$

Other results connected with Fermat's equation in the set of matrices are given in monograph [10] by P. RIBENBOIM. In these investigations it is an important problem to give a necessary and sufficient condition for the solvability of (1) in the set of matrices. Such type results were proved recently by A. KHAZANOV [7], when the matrices X, Y, Z belong to $SL_2(Z)$, $SL_3(Z)$ or $GL_3(Z)$. In particular, he proved that there are solutions of (1) in $X, Y, Z \in SL_2(Z)$ if and only if m is not a multiple of 3 or 4. We proved

in [4] a necessary condition for the solvability of (1) in 2×2 integral matrices X, Y, Z having a determinant form. More precisely, we proved (see [4], Thm. 2) that the equation (\star) does not hold in positive integers x, y, z and $m \ge 2$, if $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Another proof of this cited result was given by D. Frejman [3].

M. H. LE and CH. LI [8] proved the following generalization of our result: Let $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ be a given integral matrix such that r = Tr A = a + d > 0 and det A = ad - bc < 0, then (\star) does not hold.

In their paper they posed the following

Conjecture. Let A be an integral 2×2 matrix. The equation (\star) has a solution in natural numbers x, y, z and m > 2 if and only if the matrix A is a nilpotent matrix.

A corrected version of this Conjecture was proved by the same authors in [9].

In the present paper we prove the following

Theorem. The equation (\star) has a solution in positive integers x, y, z and m > 2 if and only if the matrix A is a nilpotent matrix or the matrix A has an eigenvalue $\alpha = \frac{1+i\sqrt{3}}{2}$.

We note that the condition matrix A has an eigenvalue $\alpha = \frac{1+i\sqrt{3}}{2}$ is equivalent to $\operatorname{Tr} A = \det A = 1$ (cf. [9]). On the other hand it is easy to see that the condition $\det A = 1$ implies that the matrix A cannot be a nilpotent matrix, thus the original Conjecture of M. H. LE and CH. Li is not true.

We also note that X. CHEN [1] proved that if A_n is the companion matrix for the polynomial $f(x) = x^n - x^{n-1} - \ldots - x - 1$ then the equation (\star) with $A = A_n$ has no solution in positive integers x, y, z and $m \geq 2$ for any fixed integer $n \geq 2$.

Futher result of this type is contained by [5]. Namely, we proved the following:

Let $A = (a_{ij})_{n \times n}$ be a matrix with at least one real eigenvalue $\alpha > \sqrt{2}$. If the equation

$$(2) A^r + A^s = A^t$$

has a solution in positive integers r, s and t then $\max\{r - t, s - t\} = -1$.

From this cited result one can obtain the corresponding results of the papers [1], [3], [4], [8] as particular cases.

2. Basic Lemmas

Lemma 1. Let $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an integral matrix such that ${\rm Tr}\, A\neq 0$ or $\det A\neq 0$ and let

$$r = a + d = \operatorname{Tr} A$$
, $s = -\det A$, $A_0 = r$, $A_1 = rA_0 + s$

and

$$A_n = rA_{n-1} + sA_{n-2} \quad \text{if} \quad n \ge 2.$$

Then for every natural number $n \geq 2$, we have

$$A^{n} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{n} = \begin{pmatrix} aA_{n-2} + sA_{n-3} & bA_{n-2} \\ cA_{n-2} & dA_{n-2} + sA_{n-3} \end{pmatrix},$$

where we put $A_{-1} = 1$.

The proof of this Lemma immediately follows from Theorem 1 of [6].

Lemma 2. Let A be an integral matrix satisfying the assumptions of Lemma 1 and let A_n be the recurrence sequence associated with the matrix A as in Lemma 1. Moreover, let Δ_n be the discriminant of the characteristic polynomial of A^n if $n \geq 2$ and let $\Delta_1 = \Delta = r^2 + 4s$. Then for every natural number $n \geq 2$ we have $\Delta_n = \Delta A_{n-2}^2$.

The proof of Lemma 2 is given in [4].

Lemma 3. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an integral matrix and let $f(x) = x^2 - (\operatorname{Tr} A)x + \det A$ be the characteristic polynomial of A with the roots $\alpha, \beta \neq \frac{1+i\sqrt{3}}{2}$ and the discriminant $\Delta = r^2 + 4s$, where $r = a + d = \operatorname{Tr} A$ and $s = -\det A$. If $s \neq 0$ and $\Delta \neq 0$ then the equation (\star) has no solutions in natural numbers x, y, z and m > 2.

Proof. If x=z and (\star) is satisfied then $A^{my}=0$, thus $\det A=0$, which contradicts to our assumption. Similarly we obtain a contradiction when y=z. If x=y then by (\star) it follows that $2A^{mx}=A^{mz}$, hence $4(\det A)^{mx}=(\det A)^{mz}$ and so we obtain a contradiction, because the last equality is impossible in natural numbers x,y,z and m>2 with integer $\det A\neq 0$.

Further on we can assume that if (\star) is satisfied, then x, y and z are distinct natural numbers. Since $s = -\det A \neq 0$, therefore there exists the inverse matrix A^{-1} and from (\star) we obtain

(3)
$$A^{m(x-z)} + A^{m(y-z)} = I$$
, if $\min\{x, y, z\} = z$

(4)
$$A^{m(x-y)} + I = A^{m(z-y)}, \text{ if } \min\{x, y, z\} = y,$$

(5)
$$I + A^{m(y-x)} = A^{m(z-x)}, \quad \text{if} \quad \min\{x, y, z\} = x,$$

where
$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
.

Let $\{A_n\}$ be the recurrence sequence associated with the matrix A. Then applying Lemma 1 to (3) we obtain

$$a\left(A_{m(x-z)-2} + A_{m(y-z)-2}\right) - (\det A)\left(A_{m(x-z)-3} + A_{m(y-z)-3}\right) = 1,$$

$$(6) \begin{array}{l} b\left(A_{m(x-z)-2} + A_{m(y-z)-2}\right) = 0, \\ c\left(A_{m(x-z)-2} + A_{m(y-z)-2}\right) = 0, \\ d\left(A_{m(x-z)-2} + A_{m(y-z)-2}\right) - (\det A)\left(A_{m(x-z)-3} + A_{m(y-z)-3}\right) = 1. \end{array}$$

From Lemma 1, (4) and (5) we obtain similar formulae to (6).

Suppose that $b \neq 0$ or $c \neq 0$. Then from (6) we get $\det A = \pm 1$. On the other hand since $\Delta \neq 0$, therefore from Lemma 2 we can deduce that

(7)
$$A_{n-2} = \frac{1}{\sqrt{\Delta}} \left(\alpha^n - \beta^n \right).$$

Substituting (7) to (6) we obtain

(8)
$$\alpha^{m(x-z)} + \alpha^{m(y-z)} = \beta^{m(x-z)} + \beta^{m(y-z)} = 1.$$

By (4) and (5) we similarly have

(9)
$$\alpha^{m(z-y)} - \alpha^{m(x-y)} = \beta^{m(z-y)} - \beta^{m(x-y)} = 1$$

and

(10)
$$\alpha^{m(z-x)} - \alpha^{m(y-x)} = \beta^{m(z-x)} - \beta^{m(y-x)} = 1.$$

From (8)–(10) it follows that in all cases

(11)
$$\alpha^{mx} + \alpha^{my} = \alpha^{mz} \text{ and } \beta^{mx} + \beta^{my} = \beta^{mz}$$

for natural numbers x, y, z and m > 2, which can be written in the forms

(12)
$$\alpha^{m(x-z)} + \alpha^{m(y-z)} = 1$$
 and $\beta^{m(x-z)} + \beta^{m(y-z)} = 1$.

Since $\Delta \neq 0$, thus we consider two cases: $\Delta > 0$ or $\Delta < 0$. Let us suppose that $\Delta > 0$. Since $\Delta = r^2 + 4s$ and $s = -\det A = \pm 1$, so we have $\Delta \geq 5$. If r > 0 then we obtain

(13)
$$\alpha = \frac{r + \sqrt{\Delta}}{2} \ge \frac{1 + \sqrt{5}}{2} > \sqrt{2} > 1.$$

From (13) and (12) it follows that both exponents m(x-z) and m(y-z) must be negative. On the other hand fom (13) we have $\alpha^{-2} < \frac{1}{2}$ and by (12) it follows that it cannot happen that both exponents m(x-z) and m(y-z) are ≤ -2 . Therefore one of them must be equal to -1 and we obtain m(x-z) = -1 or m(y-z) = -1. But this is impossible, because m > 2 and x, y, z are positive integers.

After this we consider the case $r \leq 0$. Let us suppose that r < 0 and put r = -r', where r' > 0. Then we have

$$\beta = \frac{r - \sqrt{\Delta}}{2} = -\frac{r' + \sqrt{\Delta}}{2} = -\beta$$

and

$$\beta = r' + \sqrt{\frac{\Delta}{2}} \ge \frac{1 + \sqrt{5}}{2} > \sqrt{2} > 1.$$

Substituting $\beta = -\beta$ to the second equation of (12) we obtain

(14)
$$(-1)^{m(x-z)} (\beta')^{m(x-z)} + (-1)^{m(y-z)} (\beta')^{m(y-z)} = 1.$$

If m is even then as in our previous case we obtain a contradiction. So, we can assume that m is an odd natural number greater than 2. If x - z and y - z are odd then it is easy to see that (14) does not hold. Therefore one of them must be even and from (14) we obtain

(15)
$$(\beta')^{m(x-z)} - (\beta')^{m(y-z)} = 1$$
, if $x-z$ is even and $y-z$ is odd and

(16)
$$(\beta')^{m(y-z)} - (\beta')^{m(x-z)} = 1$$
, if $y-z$ is even and $x-z$ is odd.

Because of the symmetry, it is sufficient to consider one of these equations. Let us suppose that (15) is satisfied. If x-z>0 and y-z>0 then, by(15), it follows that x-z>y-z. On the other hand, (15) can be represented in the form

(17)
$$(\beta')^{m(y-z)} \left((\beta')^{m(x-z)} - 1 \right) = 1.$$

The condition x-z>y-z implies x>y and since $\beta'>\sqrt{2}, m>2, x-z>0$ and y-z>0, therefore (17) is impossible. Hence we get that one of the differences x-z so y-z must be negative. Suppose that x-z<0 and y-z>0. Then from (15)

(18)
$$(\beta')^{m(x-z)} = (\beta')^{m(y-z)} + 1$$

follows. It is easy to see that $(\beta')^{m(x-z)} = ((\beta')^{-2})^{\frac{m(z-x)}{2}}$. On the other hand we have $(\beta')^{-2} < \frac{1}{2}$ and we obtain

$$(\beta')^{m(x-z)} = ((\beta')^{-2})^{\frac{m(z-x)}{2}} < (\frac{1}{2})^{\frac{m(z-x)}{2}} < \frac{1}{2},$$

because $\frac{m(z-x)}{2} > 1$. Therefore from (18) we get

$$(\beta')^{m(y-z)} + 1 = (\beta')^{m(x-z)} < \frac{1}{2},$$

which is impossible. In a similar way we obtain a contradiction in the case x-z>0 and y-z<0. It remains to consider the case when both differences x-z and y-z are negative. From (15) we have

(19)
$$1 = \left| (\beta')^{m(x-z)} - (\beta')^{m(y-z)} \right| \le (\beta')^{m(x-z)} + (\beta')^{m(y-z)}.$$

On the other hand we have

(20)
$$(\beta')^{m(x-z)} = ((\beta')^{-2})^{\frac{m(z-x)}{2}} < (\frac{1}{2})^{\frac{m(z-x)}{2}} < \frac{1}{2}$$

and

(21)
$$(\beta')^{m(y-z)} + \left((\beta')^{-2} \right)^{\frac{m(z-y)}{2}} < \left(\frac{1}{2} \right)^{\frac{m(z-y)}{2}} < \frac{1}{2}.$$

Hence, by (19)–(21), we get a contradiction.

Further on we have to consider the case r = 0. But in this case we have $\alpha = 1, \beta = -1$ and we can can observe that (12) is impossible.

Now, we can consider the case $\Delta < 0$. Since $s = -\det A = \pm 1$ and $\Delta = r^2 + 4s < 0$, therefore we have s = -1 and the inequality $r^2 - 4 < 0$ implies -2 < r < 2, that is, r = -1, 0, 1.

The case r = 1 is impossible by the assumptions on the eigenvalues of the matrix A.

If r = 0 then we obtain that $\alpha = i, \beta = -i$ and it is easy to check that (12) does not hold.

If r=-1 then $\alpha=\frac{-1+i\sqrt{3}}{2}$ is the third root of unity. Analyzing the exponents m(x-z) and m(y-z) modulo 3 in (12) we get a contradiction.

Summarizing, we obtain that in the case $b \neq 0$ or $c \neq 0$ the equation (\star) has no solution in positive integers x, y, z and m > 2. So, b = c = 0 and the matrix A can be reduced to a diagonal matrix of the form $A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. On the other hand for every natural number k we have

(22)
$$A^{k} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}^{k} = \begin{pmatrix} a^{k} & 0 \\ 0 & d^{k} \end{pmatrix}.$$

If (\star) is satisfied then, by (22), it follows that

(23)
$$a^{mx} + a^{my} = a^{mz}, \quad d^{mx} + d^{my} = d^{mz}.$$

From the assumption of Lemma 3 we have $s=-\det A\neq 0$. This condition implies $ad\neq 0$, because $\det A=\det \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}=ad$. Therefore (23) does not hold.

Considering all of the cases the proof of Lemma 3 is complete.

Now, we can prove the following.

Lemma 4. Let $A = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$ be an integral matrix and let $r = \operatorname{Tr} A, s = -\det A$ and $\Delta = r^2 + 4s$. If $s \neq 0$ and $\Delta = 0$, then (\star) has no solutions in positive integers x, y, z and m > 2.

Proof. Since $s \neq 0$, therefore using Lemma 1 in similar way as in the proof of Lemma 3, for the case $b \neq 0$ or $c \neq 0$ we obtain $s = -\det A = \pm 1$. Since, $\Delta = r^2 + 4s = 0$, thus s = -1 and consequently $r^2 - 4 = 0$, so we have $r = \pm 2$. Therefore we get $\alpha = \beta = \frac{r}{2} = 1$ if r = 2 and $\alpha = \beta = -1$ if r = -2. From the well-known theorem of Schur it follows that for any given matrix A there is an unitary matrix P such that

$$(24) A = P^*TP,$$

where T is the upper triangular matrix having on the main diagonal the eigenvalues of the matrix A.

Suppose that the matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with integer entries has the eigenvalues α, β .

From (24) by easy induction we obtain

$$(25) A^k = P^* T^k P$$

for every natural number k, where T^k is the upper triangular matrix with the eigenvalues α^k , β^k on the main diagonal. If (\star) is satisfied then, by (25), it follows that

$$(26) T^{mx} + T^{my} = T^{mz}$$

and from (26) we have

(27)
$$\alpha^{mx} + \alpha^{my} = \alpha^{mz}, \quad \beta^{mx} + \beta^{my} = \beta^{mz}.$$

Since in our case $\alpha = \beta = \pm 1$ so we can see that (27) does not hold. Therefore we have b = c = 0 and we get a contradiction as we have got it in the last step of the proof of Lemma 3. So the proof of Lemma 4 is complete.

Lemma 5. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an itegral matrix and let $r = \text{Tr } A, s = -\det A$ and $\Delta = r^2 + 4s$. If s = 0 and $\Delta \neq 0$ then the equation (\star) has no solution in positive integers x, y, z and m > 2.

Proof. From the assumptions of Lemma 5 it follows that $r \neq 0$ and therefore we can use Lemma 1. Since s = 0 so, by Lemma 1, it follows that

$$(28) A^k = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^k = \begin{pmatrix} ar^{k-1} & br^{k-1} \\ cr^{k-1} & dr^{k-1} \end{pmatrix} = r^{k-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = r^{k-1} A.$$

If (\star) is satisfied then from (28) we obtain

$$(29) r^{mx} + r^{my} = r^{mz}.$$

Being $r \neq 0$, it is easy to see that the equation (29) is impossible in positive integers x, y, z and m > 2. This proves Lemma 5.

3. Proof of the Theorem

Suppose that the equation (\star) has a solution in postive integers x,y,z and m>2. Then by Lemma 3, Lemma 4 and Lemma 5 it follows that $s=\det A=0$ and $r=\operatorname{Tr} A=0$ or the matrix A has an eigenvalue $\alpha=\frac{1+i\sqrt{3}}{2}$. In the case s=r=0 we have a=-d and $s=-\det A=-(ad-bc)=-\left(-d^2-bc\right)=d^2+bc=0$ and also putting d=-a we have $a^2+bc=0$. On the other hand we have

$$(30) \quad A^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & d^2 + bc \end{pmatrix} = \begin{pmatrix} a^2 + bc & br \\ cr & d^2 + bc \end{pmatrix}.$$

Substituting

$$r = 0, a^2 + bc = d^2 + bc = 0$$

to (30) we obtain that $A^2 = 0$, that is the matrix A is a nilpotent matrix with nilpotency index two.

Now, we suppose that the matrix A is nilpotent matrix, i.e. $A^k = 0$ for some natural number $k \geq 2$. Then it is easy to see that (\star) is satisfied for all positive integers x, y, z, m > 2 such that $mx \geq k, my \geq k, mz \geq k$.

Suppose that the matrix A has an eigenvalue $\alpha = \frac{1+i\sqrt{3}}{2}$. Then it is easy to check that $\alpha^2 = \frac{-1+i\sqrt{3}}{2} = \varepsilon$ is a third root of unity. By an easy calculation we obtain

(31)
$$\alpha^{n} = \begin{cases} 1, & \text{if} & n = 6k, \\ -\varepsilon^{2}, & \text{if} & n = 6k+1, \\ \varepsilon, & \text{if} & n = 6k+2, \\ -1, & \text{if} & n = 6k+3, \\ \varepsilon^{2}, & \text{if} & n = 6k+4, \\ -\varepsilon, & \text{if} & n = 6k+5. \end{cases}$$

Applying (31) we obtain that (\star) is satisfied if and only if the following relations are satisfied

(32)
$$mx \equiv r_1 \pmod{6}$$
, $my \equiv r_2 \pmod{6}$, $mz \equiv r_3 \pmod{6}$,

where

$$\langle r_1, r_2, r_3 \rangle = \langle 0, 2, 1 \rangle, \langle 0, 4, 5 \rangle, \langle 1, 3, 2 \rangle, \langle 1, 5, 0 \rangle, \langle 2, 4, 3 \rangle, \langle 2, 0, 1 \rangle,$$
$$\langle 3, 1, 2 \rangle, \langle 3, 5, 4 \rangle, \langle 4, 0, 5 \rangle, \langle 4, 2, 3 \rangle, \langle 5, 0, 1 \rangle, \langle 5, 3, 4 \rangle.$$

The proof of Theorem is complete.

From the proof of Theorem we get the following

Corollary. All soluitions of the equation(\star) in natural numbers x, y, x and m > 2, when the matrix A has an eigennvalue $\alpha = \frac{1+i\sqrt{3}}{2}$ are given by the congruence formulas (32) with the above restrictions on $\langle r_1, r_2, r_3 \rangle$ and if the matrix A is a nilpotent matrix with nilpotency index $k \geq 2$ then (\star) is satisfied by all positive integers x, y, z, m > 2 such that $mx \geq k, my \geq k$ and $mz \geq k$.

Remark. We note that Theorem with Corollary is equivalent to the result presented by M. H. Le and Ch. Li in [9], but our proof is given in another way and it gives more information about the impossibility of the solvability of (\star) in the cases mentioned in Lemma 3, 4, 5.

References

- [1] X. Chen, On Fermat's equation in the set of generalized Fibonacci matrices, Discuss. Math., Algebra and Stochastic Methods 17 (1997), 5–8.
- [2] R. Z. Domiaty, Solutions of $x^4+y^4=z^4$ in 2×2 integral matrices, Amer. Math. Monthly. **73** (1966), 631.
- [3] D. Frejman, On Fermat's equation in the set of Fibonacci matrices, *Discuss. Math.* 13 (1993), 61–64.
- [4] A. GRYTCZUK, On Fermat's equation in the set of integral 2×2 matrices, Period. Math. Hungar. 30 (1995), 67–72.
- [5] A. GRYTCZUK, Note on Fermat's type equation in the set of n×n matrices, Discuss. Math., Algebra and Stochastic Methods, 17 (1997), 19–23.
- [6] A. GRYTCZUK and K. GRYTCZUK, Functional recurrences Applications of Fibonacci Numbers, Ed. G. E. Bergum et al., by Kluwer Acad. Publ., Dordrecht, 1990, 115– 121.
- [7] A. Khazanov, Fermat's equation in matrices, Serdica Math. J. 21 (1995), 19-40.
- [8] M. H. Le and Ch. Li, A note on Fermat's equation in integral 2×2 matrices, Discuss. Math., Algebra and Stochastic Methods, 15 (1995), 135–136.
- [9] M. H. Le and Ch. Li, On Fermat's equation in integral 2×2 matrices, Period. Math. Hungar. 31 (1995), 219–222.
- [10] P.Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer Verlag, 1979.
- [11] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, Annals of Math. 141 (1995), 553–572.
- [12] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, Annals of Math. 141 (1995), 443–551.

Aleksander Grytczuk

Institute of Mathematics

DEPARTMENT OF ALGEBRA AND NUMBER THEORY

T. Kotarbinski Pedagogical University

65-069 Zielona Góra, Poland