On a conjecture about the equation

\[ A^{mx} + A^{my} = A^{mz} \]

ALEKSANDER GRYTCZUK

Abstract. Let \( A \) be a given integral \( 2 \times 2 \) 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 \( \lambda = \frac{1 + \sqrt{5}}{2} \).

1. Introduction

First we note that \((*)\) 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 \( 2 \times 2 \) integral matrices \( X, Y, Z \) for \( m = 4 \). This fact was discovered by R. Z. Domiaty [2] in 1966. Namely, he proved that, if

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

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 $2 \times 2$ integral matrices $X, Y, Z$ having a determinant form. More precisely, we proved (see [4], Thm. 2) that the equation $(\ast)$ does not hold in positive integers $x, y, z$ and $m \geq 2$, 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 C.H. 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 $r = \text{Tr} A = a + d > 0$ and $\det A = ad - bc < 0$, then $(\ast)$ does not hold.

In their paper they posed the following

**Conjecture.** Let $A$ be an integral $2 \times 2$ matrix. The equation $(\ast)$ 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 $(\ast)$ 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 $\text{Tr} A = \det A = 1$ (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

any fixed integer $n \geq 2$.

Further 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

$$A^r + A^s = A^t$$

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 $\text{Tr} A \neq 0$ or $\det A \neq 0$ and let

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

and

$$A_n = rA_{n-1} + sA_{n-2}$$

if $n \geq 2$.

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 $\Delta_n$ 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 $f(x) = x^2 - (\text{Tr} A)x + \det A$ be the characteristic polynomial of $A$ with the roots $\alpha, \beta \neq \frac{1+i\sqrt{5}}{2}$ and the discriminant $\Delta = r^2 + 4s$, where $r = a + d = \text{Tr} A$ and $s = -\det A$. If $s \neq 0$ and $\Delta \neq 0$ then the equation $(\ast)$ has no solutions in natural numbers $x, y, z$ and $m > 2$.

Proof. If $x = z$ and $(\ast)$ is satisfied then $A^{mz} = 0$, thus $\det A = 0$, which contradicts to our assumption. Similarly we obtain a contradiction when $y = z$. If $x = y$ then by $(\ast)$ it follows that $2A^{mx} = A^{mz}$, hence $4(\det A)^{nz} = (\det A)^{mx}$ 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 $(\ast)$ 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 $(\ast)$ we obtain

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

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

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

\[
\begin{align*}
\alpha (A_{m(x-z)-2} + A_{m(y-z)-2}) - (\det A) (A_{m(x-z)-3} + A_{m(y-z)-3}) &= 1, \\
b (A_{m(x-z)-2} + A_{m(y-z)-2}) &= 0, \\
c (A_{m(x-z)-2} + A_{m(y-z)-2}) &= 0, \\
d (A_{m(x-z)-2} + A_{m(y-z)-2}) - (\det A) (A_{m(x-z)-3} + A_{m(y-z)-3}) &= 1.
\end{align*}
\]

(6)

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

\[
A_{n-2} = \frac{1}{\sqrt{\Delta}} (\alpha^n - \beta^n).
\]

(7)

Substituting (7) to (6) we obtain

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

(8)

By (4) and (5) we similarly have

\[
\alpha^{m(z-y)} = \beta^{m(z-y)} - \beta^{m(x-y)} = 1
\]

and

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

(9)\( (10)\)

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

\[
\alpha^{m^x} \alpha^{m^y} = \alpha^{m^z} \text{ and } \beta^{m^x} + \beta^{m^y} = \beta^{m^z}
\]

(11)

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

\[
\alpha^{m(x-z)} + \alpha^{m(y-z)} = 1 \text{ and } \beta^{m(x-z)} + \beta^{m(y-z)} = 1.
\]

(12)

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

\[
\alpha = \frac{r + \sqrt{\Delta}}{2} \geq \frac{1 + \sqrt{5}}{2} > \sqrt{2} > 1.
\]

(13)
From (13) and (12) it follows that both exponents $m(x - z)$ and $m(y - z)$ must be negative. On the other hand from (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 $\leq -2$. 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

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

and

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

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

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

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

$$\begin{align*}
(\beta')^{m(x-z)} - (\beta')^{m(y-z)} = 1, & \quad \text{if } x - z \text{ is even and } y - z \text{ is odd} \tag{15} \\
(\beta')^{m(y-z)} - (\beta')^{m(x-z)} = 1, & \quad \text{if } y - z \text{ is even and } x - z \text{ is odd} \tag{16}
\end{align*}$$

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

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

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)

$$\begin{align*}
(\beta')^{m(x-z)} = (\beta')^{m(y-z)} + 1 \tag{18}
\end{align*}$$
follows. It is easy to see that \((\beta')^m(x-z) = \left((\beta')^{-2}\right)^{m(z-x)/2}\). On the other hand we have \((\beta')^{-2} < \frac{1}{2}\) and we obtain

\[
(\beta')^m(x-z) = \left((\beta')^{-2}\right)^{m(z-x)/2} < \left(\frac{1}{2}\right)^{m(z-x)/2} < \frac{1}{2},
\]

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

\[
1 = \left| (\beta')^m(x-z) - (\beta')^m(y-z) \right| \leq (\beta')^m(x-z) + (\beta')^m(y-z).
\]

On the other hand we have

\[
(\beta')^m(x-z) = \left((\beta')^{-2}\right)^{m(z-x)/2} < \left(\frac{1}{2}\right)^{m(z-x)/2} < \frac{1}{2}
\]

and

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

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, \(r = 1, 0, 0, 1\).

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 $(\ast)$ 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

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

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

\[(23) \quad a^{m_x} + a^{m_y} = a^{m_z}, \quad d^{m_x} + d^{m_y} = d^{m_z}.
\]

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 $r = \text{Tr} A, s = -\det A$ and $\Delta = r^2 + 4s$. If $s \neq 0$ and $\Delta = 0$, then $(\ast)$ 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

\[(24) \quad A = P^* T P,
\]

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 $\alpha, \beta$.

From (24) by easy induction we obtain

\[(25) \quad A^k = P^* T^k P
\]
for every natural number \( k \), where \( T^k \) is the upper triangular matrix with the eigenvalues \( \alpha^k, \beta^k \) on the main diagonal. If (\*) is satisfied then, by (25), it follows that

\[
T^{mx} + T^{my} = T^{mz}
\]

and from (26) we have

\[
\alpha^{mx} + \alpha^{my} = \alpha^{mz}, \quad \beta^{mx} + \beta^{my} = \beta^{mz}.
\]

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 integral 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 (\*) 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

\[
A^k = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^k = \begin{pmatrix} a r^{k-1} & b r^{k-1} \\ c r^{k-1} & d r^{k-1} \end{pmatrix} = r^{k-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = r^{k-1} A.
\]

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

\[
r^{mx} + r^{my} = r^{mz}.
\]

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

\[
A^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a^2 + bc & b(a + d) \\ c(a + d) & d^2 + bc \end{pmatrix} = \begin{pmatrix} a^2 + bc & br \\ cr & d^2 + bc \end{pmatrix}.
\]
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 (*) 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

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

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

\[
mx \equiv r_1 \pmod{6}, \quad my \equiv r_2 \pmod{6}, \quad mz \equiv r_3 \pmod{6},
\]

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 solutions of the equation (*) in natural numbers \( x, y, z \) and \( m > 2 \), when the matrix \( A \) has an eigenvalue \( \alpha = \frac{1 + i\sqrt{3}}{2} \) 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 (*) 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 C.H. LI in [9], but our proof is given in another way and it gives more information about the impossibility of the solvability of (*) in the cases mentioned in Lemma 3, 4, 5.
References


Aleksander Grytczuk

Institute of Mathematics

Department of Algebra and Number Theory

T. Kotarbinski Pedagogical University

65-069 Zielona Góra, Poland