Acta Acad. Paed. Agriensis, Sectio Mathematicae **27** *(2000) 39–46*

SOME REMARKS ON FERMAT'S EQUATION IN THE SET OF MATRICES

Zhenfu Cao (China), Aleksander Grytczuk (Poland)

Abstract. Let $\mathbf{Z}$ be the set of integers and $SL_2(\mathbf{Z})$ the set of 2×2 integral matrices with $\det A=1$ for $A\in SL_2(\mathbf{Z})$. If any two of $SL_2(\mathbf{Z})$ are commutative, then the set of such matrices we denote by $\overline{SL_2(\mathbf{Z})}$. In this paper, we prove that Fermat's equation $(*)$ $X^n+Y^n=Z^n$ has a solution in the set $\overline{SL_2(\mathbf{Z})}$ if and only if $n\equiv 1 \pmod 6$ or $n\equiv 5 \pmod 6$. This criterion is connected with a criterion given recently by Khazanov [4]. Moreover, we indicate a subclass of the matrices of $SL_2(\mathbf{Z})$ for which $(*)$ has no solutions for arbitrary positive integers $n\geq 2$.

AMS Classification Number: 11C20, 11D41

1. Introduction

Following recently results given by Wiles [8] and Taylor and Wiles [7] we know that Fermat's equation

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

has no solutions in positive integers if $n > 2$. But in contrast to this situation Fermat's equation $(*)$ has infinitely many solutions in 2×2 integral matrices for exponent $n = 4$. This fact was discovered in 1966 by Domiaty [3]. He remarked that if

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

where a, b, c are integer solutions of the Pythagorean equation $a^2 + b^2 = c^2$ then $X^4 + Y^4 = Z^4$. Another results connected with Fermat's equation in the set of matrices are described by Ribenboim in [5].

Important problem in these investigations is to give a necessary and sufficient condition for solvability of $(*)$ in the set of matrices. Let $\mathbf{Z}$ be the set of integers and $SL_2(\mathbf{Z})$ the set of 2×2 integral matrices with $\det A = 1$ for $A \in SL_2(\mathbf{Z})$. If any two of $SL_2(\mathbf{Z})$ are commutative, then the of such matrices we denote by $\overline{SL_2(\mathbf{Z})}$. Recently, Khazanov [4] find such condition for the case when the matrices

This research was partially sponsored by the Heilongjiang Province Natural Science Foundation.

$X, Y, Z \in SL_2(\mathbf{Z})$. He proved that there are solutions of $(*)$ in $X, Y, Z \in SL_2(\mathbf{Z})$ if and only if the exponent n is not multiple of 3 or 4.

In this paper, we firstly prove the following:

Theorem 1. *The Fermat's equation* $(*)$ *has a solution in* $\overline{SL_2(\mathbf{Z})}$ *if and only if* $n \equiv 1 \pmod 6$ *or* $n \equiv 5 \pmod 6$.

From Theorem 1 follows that the set of exponents n mod 12 for which $(*)$ is solvable reduce to 4 classes when $X, Y, Z \in \overline{SL_2(\mathbf{Z})}$, but if $X, Y, Z \in SL_2(\mathbf{Z})$ then Khazanov's result implies that this set has 6 classes mod 12.

Moreover, we consider the set of matrices of the following form:

$$G_2(k, \Delta) = \left\{ \begin{pmatrix} r & s \\ ks & r \end{pmatrix};\ r, s \in \mathbf{Z},\ 0 < k \in \mathbf{Z},\ \det \begin{pmatrix} r & s \\ ks & r \end{pmatrix} = \Delta \right\}, \tag{1}$$

where $k > 0, \Delta \neq 0$ are fixed integers. We note that if $\Delta = 1$ then $G_2(k, \Delta) = G_2(k, 1) \subset SL_2(\mathbf{Z})$. In [2], using Wiles' result on Fermat's last theorem, we proved

Theorem 2. *The Fermat's equation* $(*)$ *has no solutions in elements* $X, Y, Z \in G_2(k, \Delta)$ *for arbitrary positive integers* $n \geq 2$.

In this paper, we give a new proof of Theorem 2 without using a strong result of Wiles.

2. Proof of Theorem 1

In the proof of Theorem 1 we use of the following:

Lemma 1. *Let* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be a given integral matrix. Then for every natural number* $n \geq 2$

$$A^n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^n = \begin{pmatrix} F(a) & b\Psi_1 \\ c\Psi_1 & F(d) \end{pmatrix} \tag{2}$$

where $F(a) = F(a; b, c, d), F(d) = F(d; a, b, c), \Psi_1 = \Psi_1(a, b, c, d)$ *are polynomials such that*

$$F(a) - F(d) = (a - d)\Psi_1. \tag{3}$$

The proof of this Lemma is given in [1].

Now, suppose that there exists elements $X, Y, Z \in \overline{SL_2(\mathbf{Z})}$ such that

$$X^n + Y^n = Z^n. \tag{4}$$

By the assumption, we know that $\det X = \det Y = \det Z = 1$, so $Z^{-1} \in SL_2(\mathbf{Z})$ and consequently we have $XZ^{-1} = Z^{-1}X, YZ^{-1} = Z^{-1}Y$. Hence (4) is equivalent to

$$(XZ^{-1})^n + (YZ^{-1})^n = I, \tag{5}$$

where I is identity matrix and Z^{-1} is inverse matrix to Z. Let $A = XZ^{-1}$ and $B = YZ^{-1}$, then by the assumption it follows that $\det A = \det B = 1$ and (5) reduce to the equation

$$A^n + B^n = I \tag{6}$$

where $A, B \in SL_2(\mathbf{Z})$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$. Then by Lemma 1

$$A^n = \begin{pmatrix} F(a) & b\Psi_1 \\ c\Psi_1 & F(d) \end{pmatrix}, \quad B^n = \begin{pmatrix} G(e) & f\Psi_2 \\ g\Psi_2 & G(h) \end{pmatrix} \tag{7}$$

where

$$F(a) - F(d) = (a-d)\Psi_1, \quad G(e) - G(h) = (e-h)\Psi_2. \tag{8}$$

From (6) and (7) we obtain

$$F(a) + G(e) = F(d) + G(h) = 1, \quad b\Psi_1 + f\Psi_2 = c\Psi_1 + g\Psi_2 = 0. \tag{9}$$

Since $\det A = \det B = 1$ then by Cauchy's theorem on product of determinants follows $\det A^n = \det B^n = 1$ and consequently from (7) we get

$$F(a)F(d) - bc\Psi_1^2 = G(e)G(h) - gf\Psi_2^2 = 1. \tag{10}$$

From (9) we have $b\Psi_1 = -f\Psi_2$ and $c\Psi_1 = -g\Psi_2$, thus $bc\Psi_1^2 = fg\Psi_2^2$. By the last equality and (10), it follows that

$$F(a)F(d) = G(e)G(h). \tag{11}$$

On the other hand from (9) we have $F(a) = 1 - G(e)$ and $F(d) = 1 - G(h)$ and substitutting to (11) we obtain

$$G(e) + G(h) = 1. \tag{12}$$

From (12) and the fact that $F(a) + F(d) = 2 - (G(e) + G(h))$ follows

$$F(a) + F(d) = 1. \tag{13}$$

From (13) and (12) we have

$$TrA^n = F(a) + F(d) = 1, \quad TrB^n = G(e) + G(h) = 1. \tag{14}$$

Let α, β be the eigenvalues of the matrix A. Then it is well-known that the matrix A^n has eigenvalues α^n, β^n such that

$$TrA^n = \alpha^n + \beta^n, \quad \det A^n = \alpha^n \beta^n. \tag{15}$$

By (15) and (14) it follows that

$$\alpha^n + \beta^n = 1, \quad \alpha^n \beta^n = 1. \tag{16}$$

From (16) we obtain

$$\alpha^{2n} - \alpha^n + 1 = 0. \tag{17}$$

Let $\alpha^n = x$ then (17) reduce to quadratic equation with the following complex roots

$$x_1 = \frac{1 + i\sqrt{3}}{2}, x_2 = \bar{x}_1 = \frac{1 - i\sqrt{3}}{2}. \tag{18}$$

Now, we observe that the condition $\alpha^n = x_1, x_2$, where x_1, x_2 are given by (18) implies that α is a complex number. Sincce $\alpha = \frac{a+d+\sqrt{(a+d)^2-4\det A}}{2}$ and $\det A = 1$ then $(a+d)^2 - 4 < 0$ so is equivalent to $-2 < a + d < 2$. Hence it remains to consider three following cases: 1. $a + d = -1$; 2. $a + d = 0$; 3. $a + d = 1$.

In the first case we have $\alpha = \frac{-1+i\sqrt{3}}{2}$ is the root of unity of degree 3. If we consider the exponent n with respect to modulo 6 then we get $\alpha^{6k} = 1 \neq x_1, x_2; \alpha^{6k-1} = \alpha \neq x_1, x_2; \alpha^{6k+2} = \alpha^2 = \frac{-1-i\sqrt{3}}{2} \neq x_1, x_2; \alpha^{6k+3} = \alpha^3 = 1 \neq x_1, x_2$; $\alpha^{6k+4} = \alpha \neq x_1, x_2$ and $\alpha^{6k+5} = \alpha^2 = \frac{-1-i\sqrt{3}}{2} \neq x_1, x_2$. Hence in this case the equation (6) is impossible.

Suppose that case 2 is satisfied. Then we have $\alpha = i$ and by similar way considering the exponent n with respect to modulo 4 we obtain in all cases that $\alpha^n = i^n \neq x_1, x_2$.

It remains to consider the last case, i.e. $a + d = 1$. In this case we have $\alpha = \frac{1+i\sqrt{3}}{2}$ and consequently the equality $\alpha^n = x_1, x_2$ is possible when $n \equiv 1 \pmod 6$ or $n \equiv 5 \pmod 6$.

Now, suppose that $n \equiv 1 (\text{mod } 6)$ or $n \equiv 5 (\text{mod } 6)$. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be the integral matrix such that $TrM = \det M = 1$. It is easy to see that this condition is equivalent to that the matrix M has eigenvalues: $\alpha = \frac{1+i\sqrt{3}}{2}, \beta = \frac{1-i\sqrt{3}}{2}$. Put $A = M^x, B = M^y, C = I^z$. Then by the condition $\det M = 1$ follows $\det A = \det B = \det C = 1$ so the matrices $A, B, C \in SL_2(\mathbf{Z})$. On the other hand since $\alpha \neq \beta$ then the matrix M is diagonalizable over the complex field. Hence there is a nonsigular matrix P such that $M = PDP^{-1}$, where $D = \text{diag}\{\alpha, \beta\}$. By induction it follows that for every natural number k we have

$$M^k = PD^kP^{-1} = P\text{diag}\{\alpha^k, \beta^k\}P^{-1}. \tag{19}$$

Using (19) we obtain that equation (6) is equivalent to

$$\alpha^{nx} + \alpha^{ny} = 1, \quad \beta^{nx} + \beta^{ny} = 1. \tag{20}$$

Since $\alpha = \frac{1+i\sqrt{3}}{2}$ then $\alpha^2 = \frac{-1+i\sqrt{3}}{2} = \epsilon_1$, where ϵ_1 is the root of unity of degree 3. Similarly we obtain that $\beta^2 = \left(\frac{1-i\sqrt{3}}{2}\right)^2 = \frac{-1-i\sqrt{3}}{2} = \epsilon_2 = \bar{\epsilon}_1$.

On the other hand we observe that if ϵ is the root of unity of degree 3 then we have

$$\alpha^m = \begin{cases} 1, & \text{if } m = 6k, \\ -\epsilon^2, & \text{if } m = 6k+1, \\ \epsilon, & \text{if } m = 6k+2, \\ -1, & \text{if } m = 6k+3, \\ \epsilon^2, & \text{if } m = 6k+4, \\ -\epsilon, & \text{if } m = 6k+5. \end{cases} \tag{21}$$

where in (21) $\epsilon = \epsilon_1$ when $\alpha = \frac{1+i\sqrt{3}}{2}$ and α is replaced by β and $\epsilon = \epsilon_2$ in other case.

Let $n \equiv 1 \pmod 6$. Then we take $x \equiv 1 \pmod 6$ and $y \equiv 5 \pmod 6$ or $x \equiv 5 \pmod 6$ and $y \equiv 1 \pmod 6$. Hence we have $nx \equiv 1 \pmod 6$ and $ny \equiv 5 \pmod 6$ or $nx \equiv 5 \pmod 6$ and $ny \equiv 1 \pmod 6$. From (21) it follows that in these cases we have

$$\alpha^{nx} + \alpha^{ny} = -\epsilon^2 - \epsilon = 1,$$

because $\epsilon^2 + \epsilon + 1 = 0$. In similar way we obtain

$$\beta^{nx} + \beta^{ny} = 1.$$

Hence equation (6) has a solution in elements $A, B, C \in SL_2(\mathbf{Z})$ if $n \equiv 1 \pmod 6$.

Let us suppose that $n \equiv 5 \pmod 6$. Taking $x \equiv 1 \pmod 6$, $y \equiv 5 \pmod 6$ or $x \equiv 5 \pmod 6$, $y \equiv 1 \pmod 6$ we obtain $nx \equiv 5 \pmod 6$, $ny \equiv 1 \pmod 6$ or $nx \equiv 1 \pmod 6$, $ny \equiv 5 \pmod 6$. Hence, we see that we have the same case as in the previous consideration. The proof of Theorem 1 is complete.

3. Proof of Theorem 2

Let $X, Y, Z \in G_2(k, \Delta)$ and let

$$X = \begin{pmatrix} r_1 & s_1 \\ ks_1 & r_1 \end{pmatrix}, \quad Y = \begin{pmatrix} r_2 & s_2 \\ ks_2 & r_2 \end{pmatrix}, \quad Z = \begin{pmatrix} r_3 & s_3 \\ ks_3 & r_3 \end{pmatrix}.$$

Then we have $Z^{-1} = \frac{1}{\Delta}\begin{pmatrix} r_3 & -s_3 \\ -ks_3 & r_3 \end{pmatrix}$. Suppose that for some natural number $n \geq 2$ we have $X^n + Y^n = Z^n$. Then multyplying the last equation by Z^{-n} we get

$$(XZ^{-1})^n + (YZ^{-1})^n = I, \tag{22}$$

because $XZ^{-1} = Z^{-1}X$ and $YZ^{-1} = Z^{-1}Y$. On the other hand we have

$$XZ^{-1} = \begin{pmatrix} r_1 & s_1 \\ ks_1 & r_1 \end{pmatrix} \frac{1}{\Delta} \begin{pmatrix} r_3 & -s_3 \\ -ks_3 & r_3 \end{pmatrix}$$

$$= \frac{1}{\Delta} \begin{pmatrix} r_1r_3 - ks_1s_3 & s_1r_3 - r_1s_3 \\ k(s_1r_3 - r_1s_3) & r_1r_3 - ks_1s_3 \end{pmatrix} = \frac{1}{\Delta} \begin{pmatrix} R & S \\ kS & R \end{pmatrix} = \frac{1}{\Delta} A \tag{23}$$

and

$$YZ^{-1} = \begin{pmatrix} r_2 & s_2 \\ ks_2 & r_2 \end{pmatrix} \frac{1}{\Delta} \begin{pmatrix} r_3 & -s_3 \\ -ks_3 & r_3 \end{pmatrix}$$

$$= \frac{1}{\Delta} \begin{pmatrix} r_2r_3 - ks_2s_3 & s_2r_3 - r_2s_3 \\ k(s_2r_3 - r_2s_3) & r_2r_3 - ks_2s_3 \end{pmatrix} = \frac{1}{\Delta} \begin{pmatrix} M & N \\ kN & M \end{pmatrix} = \frac{1}{\Delta} B. \tag{24}$$

From (22)–(24) we obtain

$$A^n + B^n = \Delta^n I = \begin{pmatrix} \Delta^n & 0 \\ 0 & \Delta^n \end{pmatrix}. \tag{25}$$

On the other hand we have

$$A^n = \begin{pmatrix} R & S \\ kS & R \end{pmatrix}^n = \begin{pmatrix} R_n & S_n \\ kS_n & R_n \end{pmatrix}, B^n = \begin{pmatrix} M & N \\ kN & M \end{pmatrix}^n = \begin{pmatrix} M_n & N_n \\ kN_n & M_n \end{pmatrix}. \tag{26}$$

From (25) and (26) we obtain

$$R_n + M_n = \Delta^n, S_n + N_n = 0 \tag{27}$$

because $k > 0$. It is easy to check that

$$\det A = \det \begin{pmatrix} R & S \\ kS & R \end{pmatrix} = \det \begin{pmatrix} r_1 & s_1 \\ ks_1 & r_1 \end{pmatrix} \det \begin{pmatrix} r_3 & -s_3 \\ -ks_3 & r_3 \end{pmatrix} = \Delta^2.$$

Similarly we get $\det B = \Delta^2$. Hence by Cauchy's theorem it follows that

$$\det A^n = (\det A)^n = \Delta^{2n}, \quad \det B^n = (\det B)^n = \Delta^{2n}. \tag{28}$$

From (26) we have

$$\det A^n = R_n^2 - kS_n^2, \quad \det B^n = M_n^2 - kN_n^2. \tag{29}$$

By (28) and (29) it follows that

$$R_n^2 - M_n^2 = k(S_n^2 - N_n^2) = k(S_n - N_n)(S_n + N_n). \tag{30}$$

But from (27) we have $S_n + N_n = 0$ and therefore by (30) it follows that

$$R_n^2 - M_n^2 = (R_n - M_n)(R_n + M_n) = 0. \tag{31}$$

Since by (27) $R_n + M_n = \Delta^n \neq 0$, then from (31) we obtain that $R_n = M_n$ so $2R_n = \Delta^n$. From (28), (29) and the last equality we get

$$3\Delta^{2n} = -k(2S_n)^2 \tag{32}$$

and we see that (32) is impossible, because $\Delta \neq 0$ and $k > 0$.

The proof of Theorem 2 is complete.

Remark. Let $K = Q(\sqrt{k})$ be quadratic number field with $k > 0$ and $k \equiv 2, 3 \pmod 4$. Then it is well-known that every integer element α in such field has the form: $\alpha = r + s\sqrt{k}$, where $r, s \in \mathbf{Z}$. Denote by R_K the ring of integer elements of this field K and by $G_2(k)$ the set of matrices of the form:

$$G_2(k) = \left\{ \begin{pmatrix} r & s \\ ks & r \end{pmatrix}; r, s \in \mathbf{Z}, 0 < k \in \mathbf{Z}, k \equiv 2, 3 \pmod 4 \right\}.$$

It is easy to see that the mapping $\Phi : G_2(k) \to R_K$ defined by the formula

$$\Phi\left(\begin{pmatrix} r & s \\ ks & r \end{pmatrix} \right) = r + s\sqrt{k}$$

is an isomorphism. Hence from Theorem 2 we obtain the following:

Corollary. *The Fermat's equation $\alpha^n + \beta^n = \gamma^n, n \geq 2$ has no solutions in elements $\alpha, \beta, \gamma \in R_K$ with the same norm, i.e. if $N(\alpha) = N(\beta) = N(\gamma) = \Delta$.*

References

[1] Bialek, K. and Grytczuk, A., The equation of Fermat in $G_2(k)$ and $Q(\sqrt{k})$, *Acta Acad. Paed. Agriensis-Sectio Mat. Eger.*, **13** (1987), 81–90.

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

[3] Domiaty, R., Solution of $x^4 + y^4 = z^4$ in 2×2 integral matrices, *Amer. Math. Monthly*, **73** (1966), 631.

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

[5] Ribenboim, P., 13 Lectures on Fermat's Last Theorem, Springer Verlag, 1979.

[6] Rotkiewicz, A., Applications of Jacobi's symbol to Lehmer's numbers, *Acta Arith.*, **42** (1983), 163–187.

[7] Taylor, R. and Wiles, A., Ring-theoretic properties of certain Hecke algebras, *Annals of Math.*, **141** (1995), 553–572.

[8] Wiles, A., Modular elliptic curves and Fermat's Last Theorem, *Annals of Math.*, **141** (1995), 443–551.

Zhenfu Cao
Department of Mathematics
Harbin Institute of Technology
Harbin 150001
P. R. China
e-mail: zfcao@hope.hit.edu.cn

Aleksander Grytczuk
Institute of Mathematics
Department of Algebra and Number Theory
T. Kotarbiński Pedagogical University
65-069 Zielona Góra, Poland