TSUKUBA J. MATH.
Vol. 22 No. 3 (1998), 637-643

FERMAT'S TYPE EQUATIONS IN THE SET OF 2×2 INTEGRAL MATRICES

By

Zhenfu CAO and Aleksander GRYTCZUK

1. Introduction.

Following recently result given by Wiles [6] we know that the equation of Fermat $(*)$ $X^n + Y^n = Z^n$ has no solutions in positive integers X, Y, Z if $n > 2$. But in contrast to this situation Fermat's equation $(*)$ has infinitely many solutions in 2×2 integer matrices for exponent $n = 4$. This fact has been discovered by Domiaty [2] in 1996. Namely, he remarked that if

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

where a, b, c are the 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 [5]. Important problem in these investigations is to give a necessary and sufficient condition for solvability $(*)$ in the set of matrices. Second Author proved (see; [3], Thm. 1) a necessary condition for solvabilty $(*)$ in the set of 2×2 integral matrices. Moreover, Khazanov [4] founded a necessary and sufficient condition for solvabilty $(*)$ when $X, Y, Z \in SL_2(Z)$, $SL_3(Z)$, or $GL_3(Z)$. In particular, he proved that there are solutions of $(*)$ in $X, Y, Z \in SL_2(Z)$ if and only if the exponent n is not a multiple of 3 or 4. In this connection we consider the following set of integer matrices:

$$G(k, \pm 1) = \left\{ \begin{pmatrix} r & s \\ ks & r \end{pmatrix};\ r, s \in Z,\ \det\begin{pmatrix} r & s \\ ks & r \end{pmatrix} = \pm 1 \right\},$$

where k is a fixed positive integer which is not a perfect square.

We note that if $k < 0$ or $k = a^2$, $a \in Z$ then the condition $\det\begin{pmatrix} r & s \\ ks & r \end{pmatrix} = r^2 - ks^2 = \pm 1$ implies $s = 0$, $r = \pm 1$ and the set $G(k, \pm 1)$ reduces to trivial set:

Received July 7, 1997
Revised January 13, 1998

$G_0(k, \pm 1) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$. But if $k > 0$ and $k \neq a^2$, $a \in Z$ then the set $G(k, \pm 1)$ is an infinite set. On the other hand it is easy to see that if $\det\begin{pmatrix} r & s \\ ks & r \end{pmatrix} = 1$ then the set $G(k, 1)$ is a subset of $SL_2(Z)$ considered by Khazanov in [4]. We prove the following:

THEOREM 1. *The equation of Fermat* $(*)$ *has no solutions in* $X, Y, Z \in G(k, \pm 1)$ *for any positive integer* n.

Moreover, we consider more general situation when $G(k, a)$ is the set of the form:

$$G(k, a) = \left\{ \begin{pmatrix} r & s \\ ks & r \end{pmatrix}, r, s \in Z;\ \det\begin{pmatrix} r & s \\ ks & r \end{pmatrix} = a \right\},$$

where k is a fixed positive integer and a is a fixed integer.

We prove of the following:

THEOREM 2. *If* $X, Y, Z \in G(k, a)$ *then the equation of Fermat* $(*)$ *with positive integer exponent* $n \geq 3$ *does not hold, except when* $X = O$ or $Y = O$ or $Z = O$.

Further, we prove

THEOREM 3. *If* $X, Y, Z, W \in G(k, a)$ *and* $k > 1$ *is a fixed square-free integer then the equation*:

$$(**) \qquad X^n + Y^n + Z^n = W^n; \quad n \geq 1$$

does not hold, except when $X + Y = O$ *or* $Y + Z = O$ *or* $Z + X = O$ *and* $(n, 2) = 1$.

2. Lemmas.

In the proof of our results we use of the following:

LEMMA 1. *For any positive integer* n *we have*

$$(1) \qquad \begin{pmatrix} r & s \\ ks & r \end{pmatrix}^n = \begin{pmatrix} R_n & S_n \\ kS_n & R_n \end{pmatrix},$$

where

$$(2)\qquad R_n=\frac{1}{2}(\alpha^n+\beta^n),\quad S_n=\frac{1}{2\sqrt{k}}(\alpha^n-\beta^n),\quad \alpha=r+s\sqrt{k},\quad \beta=r-s\sqrt{k}.$$

PROOF. The proof of (1) follows by the following equality:

$$\begin{pmatrix} r_1 & s_1\\ ks_1 & r_1\end{pmatrix}\begin{pmatrix} r_2 & s_2\\ ks_2 & r_2\end{pmatrix}=\begin{pmatrix} r_1r_2+ks_1s_2 & r_1s_2+s_1r_2\\ k(r_1s_2+s_1r_2) & r_1r_2+ks_1s_2\end{pmatrix}=\begin{pmatrix} R & S\\ kS & S\end{pmatrix}.$$

Let $A=\begin{pmatrix} r & s\\ ks & r\end{pmatrix}$, then by easy calculation we obtain that $\alpha=r+s\sqrt{k}$ and $\beta=r-s\sqrt{k}$ are the eigenvalues of the matrix A. On the other hand it is well-known that the matrix A^n has the eigenvalues α^n and β^n such that

$$(3)\qquad TrA^n=\alpha^n+\beta^n,\quad \det A^n=\alpha^n\beta^n.$$

From (3) and (1) we obtain (2) and the proof of Lemma 1 is complete.

Moreover, we use of the following:

LEMMA 2. *Let $r_1,r_2,r_3\in Z$ and $n\geq 3$ be a positive integer. If $r_1^n+r_2^n=r_3^n$ then $r_1r_2r_3=0$.*

The proof of Lemma 2 follows by the result of Wiles [6].

3. Proof of Theorem 1.

Suppose that the equation $(*)$ $X^n+Y^n=Z^n$ has a solution in the elements $X,Y,Z\in G(k,\pm 1)$ and let $X=\begin{pmatrix} r_1 & s_1\\ ks_1 & r_1\end{pmatrix}$, $Y=\begin{pmatrix} r_2 & s_2\\ ks_2 & r_3\end{pmatrix}$ and $Z=\begin{pmatrix} r_3 & s_3\\ ks_3 & r_3\end{pmatrix}$. Then we have $\det X$, $\det Y$, $\det Z\in\{\pm 1\}$ and $\det X=\det Y=\det Z$. From the theory of the equation $u^2-kv^2=\pm 1$ we know (see; e.g. [2]) that $r_i+s_i\sqrt{k}=\varepsilon^{m_i}$, $i=1,2,3$ where $\varepsilon=u_0^{(i)}+v_0^{(i)}\sqrt{k}$ is the fundamental solution of the non-Pellian equation $u^2-kv^2=-1$ when this equation is solvable in integers u,v or otherwise ε is the fundamental solution of the Pell equation $u^2-kv^2=1$. By Lemma 1 it follows that

$$X^n=\begin{pmatrix} R_n^{(1)} & S_n^{(1)}\\ kS_n^{(1)} & R_n^{(1)}\end{pmatrix},\quad Y^n=\begin{pmatrix} R_n^{(2)} & S_n^{(2)}\\ kS_n^{(2)} & R_n^{(2)}\end{pmatrix},\quad Z^n=\begin{pmatrix} R_n^{(3)} & S_n^{(3)}\\ kS_n^{(3)} & R_n^{(3)}\end{pmatrix}$$

where

(4) $$R_n^{(i)} = \frac{1}{2}(\alpha_i^n + \beta_i^n), \quad S_n^{(i)} = \frac{1}{2\sqrt{k}}(\alpha_i^n - \beta_i^n), \quad i = 1,2,3$$

and

(5) $$\alpha_i = r_i + s_i\sqrt{k} = \varepsilon^{m_i}, \quad \beta_i = r_i - s_i\sqrt{k} = (\varepsilon^{-1})^{m_i}, \quad i = 1,2,3$$

(6) $$\varepsilon = u_0 + v_0\sqrt{k}, \quad \varepsilon^{-1} = u_0 - v_0\sqrt{k}.$$

From the assumption that $X^n + Y^n = Z^n$ it follows that

(7) $$R_n^{(1)} + R_n^{(2)} = R_n^{(3)}, \quad S_n^{(1)} + S_n^{(2)} = S_n^{(3)}.$$

By (4) and (7) it follows that

(8) $$\alpha_1^n + \beta_1^n + \alpha_2^n + \beta_2^n = \alpha_3^n + \beta_3^n$$

(9) $$\alpha_1^n - \beta_1^n + \alpha_2^n - \beta_2^n = \alpha_3^n - \beta_3^n.$$

From (8) and (9) we obtain

(10) $$\alpha_1^n + \alpha_2^n = \alpha_3^n, \quad \beta_1^n + \beta_2^n = \beta_3^n.$$

By (10) and (5) it follows that

(11) $$\varepsilon^{nm_1} + \varepsilon^{nm_2} = \varepsilon^{nm_3}.$$

It is clear that $m_3 \geq \max\{m_1, m_2\}$ and we can assume without loss of generality that $m_1 \leq m_2$. Then by (11) it follows that

(12) $$1 + \varepsilon^{n(m_2-m_1)} = \varepsilon^{n(m_3-m_1)}.$$

Put $\varepsilon^t = a_t + b_t\sqrt{k}$ for non-negative integers t. Then it is easy to see that a_t and b_t are non-negative integers and from (12) we obtain

$$1 + a_{n(m_2-m_1)} + b_{n(m_2-m_1)}\sqrt{k} = a_{n(m_3-m_1)} + b_{n(m_3-m_1)}\sqrt{k}.$$

Hence, from the last equality we have

(13) $$1 + a_{n(m_2-m_1)} = a_{n(m_3-m_1)}$$

(14) $$b_{n(m_2-m_1)} = b_{n(m_3-m_1)}.$$

By (14) follows that $m_2 = m_3$ and consequently from (13) we get a contradiction. The proof of the Theorem 1 is complete.

3. Proof of Theorem 2.

Suppose that $X = \begin{pmatrix} r_1 & s_1 \\ ks_1 & r_1 \end{pmatrix}$, $Y = \begin{pmatrix} r_2 & s_2 \\ ks_2 & r_2 \end{pmatrix}$, $Z = \begin{pmatrix} r_3 & s_3 \\ ks_3 & r_3 \end{pmatrix}$ is a solution of $(*)$ with $\det X = \det Y = \det Z = a$. Then by Lemma 1 in similar way as in the proof of Theorem 1 we obtain

$$X^n = \begin{pmatrix} R_n^{(1)} & S_n^{(1)} \\ kS_n^{(1)} & R_n^{(1)} \end{pmatrix}, \quad Y^n = \begin{pmatrix} R_n^{(2)} & S_n^{(2)} \\ kS_n^{(2)} & R_n^{(2)} \end{pmatrix}, \quad Z^n = \begin{pmatrix} R_n^{(3)} & S_n^{(3)} \\ kS_n^{(3)} & R_n^{(3)} \end{pmatrix}$$

and

$$R_n^{(i)} = \frac{1}{2}(\alpha_i^n + \beta_i^n), \quad S_n^{(i)} = \frac{1}{2\sqrt{k}}(\alpha_i^n - \beta_i^n), \quad \alpha_i = r_i + s_i\sqrt{k}, \quad \beta_i = r_i - s_i\sqrt{k}; \ i = 1,2,3.$$

Thus by the assumption we have

$$R_n^{(1)} + R_n^{(2)} = R_n^{(3)}, \quad S_n^{(1)} + S_n^{(2)} = S_n^{(3)} \tag{15}$$

and consequently we obtain

$$\alpha_1^n + \alpha_2^n = \alpha_3^n, \quad \beta_1^n + \beta_2^n = \beta_3^n. \tag{16}$$

On the other hand we have $\det X = \det Y = \det Z = a = r_i^2 - ks_i^2 = \alpha_i\beta_i$ for $i = 1,2,3$. But from (16) we get $(\alpha_1^n + \alpha_2^n)(\beta_1^n + \beta_2^n) = (\alpha_3\beta_3)^n$ and consequently we obtain

$$a^n + (\alpha_1\beta_2)^n + (\alpha_2\beta_1)^n = 0. \tag{17}$$

If $a = 0$ then $\alpha_i = 0$ or $\beta_i = 0$ and we have $R_n^{(i)} = 2^{n-1}r_i^n$ for $i = 1,2,3$. Hence, by (15) it follows that

$$r_1^n + r_2^n = r_3^n \tag{18}$$

From (18) and Lemma 2 we get that $r_1r_2r_3 = 0$, because $r_1, r_2, r_3 \in Z$. This fact implies that $X = O$ or $Y = O$ or $Z = O$. Now, we can assume that $a \neq 0$.

Since $a = \alpha_1\beta_1 = \alpha_2\beta_2$ then by (17) it follows that

$$1 + \left(\frac{\beta_2}{\beta_1}\right)^n + \left(\frac{\beta_1}{\beta_2}\right)^n = 0. \tag{19}$$

Putting $(\beta_2/\beta_1)^n = x$ in the equality (19) we obtain the equation $x^2 + x + 1 = 0$. It is easy to observe that $x = (-1 \pm \sqrt{-3})/2$ and consequently we obtain that $(\beta_2/\beta_1)^n = (-1 \pm \sqrt{-3})/2$. But the last equality is impossible for any positive integer $n \geq 1$. The proof of the Theorem 2 is complete.

4. Proof of Theorem 3.

Suppose that

$$X = \begin{pmatrix} r_1 & s_1 \\ ks_1 & r_1 \end{pmatrix}, \quad Y = \begin{pmatrix} r_2 & s_2 \\ ks_2 & r_2 \end{pmatrix}, \quad Z = \begin{pmatrix} r_3 & s_3 \\ ks_3 & r_3 \end{pmatrix}, \quad W = \begin{pmatrix} r_4 & s_4 \\ ks_4 & r_4 \end{pmatrix},$$

where $\det X = \det Y = \det Z = \det W = a$ is a solution of the equation $(**)$. First, we note that since $k > 1$ is a square-free integer then the condition $a = 0$ implies $X = Y = Z = W = O$. Thus, we can assume that $a \neq 0$. Using Lemma 1 by similar way as in the proof of the Theorem 2 we obtain

$$\alpha_1^n + \alpha_2^n + \alpha_3^n = \alpha_4^n, \quad \beta_1^n + \beta_2^n + \beta_3^n = \beta_4^n \tag{20}$$

Since $\det X = \det Y = \det Z = \det W = a = r_i^2 - ks_i^2 = \alpha_i\beta_i$; $i = 1, 2, 3$ then by (20) it follows that

$$2a^n + (\alpha_1\beta_2)^n + (\alpha_1\beta_3)^n + (\alpha_2\beta_1)^n + (\alpha_2\beta_3)^n + (\alpha_3\beta_1)^n + (\alpha_3\beta_2)^n = 0. \tag{21}$$

One the other hand we have $a \neq 0$ and $\alpha_i = (a/\beta_i)$ for $i = 1, 2, 3$ thus from (21) we get

$$2 + \left(\frac{\beta_2}{\beta_1}\right)^n + \left(\frac{\beta_3}{\beta_1}\right)^n + \left(\frac{\beta_1}{\beta_2}\right)^n + \left(\frac{\beta_3}{\beta_2}\right)^n + \left(\frac{\beta_1}{\beta_3}\right)^n + \left(\frac{\beta_2}{\beta_3}\right)^n = 0. \tag{22}$$

Denoting by $x_1 = (\beta_2/\beta_1)^n$, $x_2 = (\beta_3/\beta_2)^n$ and $x_3 = (\beta_1/\beta_3)^n$ we obtain $x_1x_2x_3 = 1$ and consequently the equation (22) reduces to the following equation:

$$2 + x_1 + x_2 + x_3 + x_1x_2 + x_2x_3 + x_3x_1 = 0. \tag{23}$$

Since $x_1x_2x_3 = 1$ then by (23) it follows that $x_1 = -1$ or $x_2 = -1$ or $x_3 = -1$. By the symmetry of (23) we can assume without loss of generality that $x_1 = -1$. Since $\beta_1 = r_1 - s_1\sqrt{k}$, $\beta_2 = r_2 - s_2\sqrt{k}$ and $x_1 = (\beta_2/\beta_1)^n$ then we obtain

$$\left(\frac{r_2 - s_2\sqrt{k}}{r_1 - s_1\sqrt{k}}\right)^n = -1. \tag{24}$$

It is easy to see that if the exponent n is an even positive integer then the equation (24) is impossible. Suppose that n is an odd positive integer, so $(n, 2) = 1$. Then from (24) we obtain

$$((r_1r_2 - ks_1s_2) + (s_1r_2 - r_1s_2)\sqrt{k})^n = (-a)^n. \tag{25}$$

Since $k > 1$ is a square-free integer then by (25) it follows that

$$r_1r_2 - ks_1s_2 = -a, \quad s_1r_2 - r_1s_2 = 0. \tag{26}$$

From (26) we obtain $r_2 = -r_1$ and $s_2 = -s_1$ and therefore we have

$$X + Y = \begin{pmatrix} r_1 & s_1 \\ ks_1 & r_1 \end{pmatrix} + \begin{pmatrix} r_2 & s_2 \\ ks_2 & r_2 \end{pmatrix} = \begin{pmatrix} r_1 + r_2 & s_1 + s_2 \\ k(s_1 + s_2) & r_1 + r_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O.$$

The proof of Theorem 3 is complete.

REMARK. Similar result to the Theorem 3 one can obtain for the following equation $X_1^n + X_2^n + \cdots + X_m^n = Y^n$, when $X_1, X_2, \ldots, X_m, Y \in G(k,a)$ and $k > 1$ is a fixed square-free integer and $n \geq 1$, $m \geq 2$ are arbitrary fixed integers.

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

References.

[1] Z. F. Cao, Introduction to Diophantine equations, Harbin Institute Techn., 1989

[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), 67–72.

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

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

[6] A. Wiles, 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, PR
China

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

1991-Mathematics Subject Classification-11C20, 11D41