RESEARCH ARTICLE
doi: 10.2306/scienceasia1513-1874.2013.39.653

ScienceAsia 39 (2013): **653–655**

On some Diophantine problems in 2×2 integer matrices

Walisa Intrarapak, Supawadee Prugsapitak*

Department of Mathematics and Statistics, Faculty of Science, Prince of Songkla University, Hatyai, Songkla 90110 Thailand

*Corresponding author, e-mail: supawadee.p@psu.ac.th

Received 21 Sep 2012
Accepted 13 Nov 2013

ABSTRACT: Let F be an algebraic number field with O_F its ring of algebraic integers. We find a condition for which the equation $aX^n + bY^n = cZ^n$ where $a, b, c \in O_F$ does not hold over a 2×2 matrix ring over a ring of algebraic integers.

KEYWORDS: Fermat's equation, 2×2 matrix

INTRODUCTION

Wiles[1] proved that Fermat's equation,

$$X^n + Y^n = Z^n, \tag{1}$$

has no solution in positive integers if $n \geqslant 3$. In the matrix case, the answer is different. Domiaty[2] gave solutions of $x^4 + y^4 = z^4$ with x, y, z of the form

$$\begin{pmatrix} 0 & * \\ 1 & 0 \end{pmatrix}.$$

Li and Le[3] proved a necessary and sufficient condition for solvability of (1) for $n > 2$ over the set $\mathbb{A} = \{A^k \mid k \in \mathbb{N}\}$ where A is a 2×2 matrix. Cao and Grytzuk[4] showed that (1) has no solutions over the set

$$G(k, d) = \left\{ \begin{pmatrix} e & f \\ kf & e \end{pmatrix} \,\middle|\, e, f \in \mathbb{N}, \begin{vmatrix} e & f \\ kf & e \end{vmatrix} = d \right\}$$

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

It is natural to ask about the solvability of the Fermat-like equation,

$$aX^n + bY^n = cZ^n \tag{2}$$

over 2×2 integer matrices. Moreover, since the set of integers is the ring of integers of the field of rational numbers, it is natural to ask about a solvability of (2) over a ring of a 2×2 matrix over a ring of integers of a number field. Our objective here is to show some conditions on a 2×2 matrix so that (2) does not hold over a ring of algebraic integers.

MAIN RESULTS

We consider the equation

$$aX^n + bY^n = cZ^n \tag{3}$$

where $X, Y, Z \in \mathbb{A}$, $n \in \mathbb{N}$, $n > 2$.

Theorem 1 *Let*

$$A = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

be an integer matrix having two distinct non-zero real eigenvalues α and β and $\alpha > 1$. Let a, b, c be positive integers such that $a \geqslant b \geqslant c$. Then (3) has no solution (X, Y, Z, n) for every natural number $n > N$ where

$$N = \frac{\log \lceil a/c \rceil + \log 2}{\log \alpha}.$$

Proof: Let

$$A = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

be an integer matrix having two distinct non-zero real eigenvalues α and β and $\alpha > 1$. Then there exists a nonsingular matrix P such that $A = P^{-1}DP$ where

$$D = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.$$

By induction, we have $A^k = P^{-1}D^kP$ for $k \geqslant 1$. Suppose on the contrary that for some $n > N$, (3) holds, i.e., $aA^{kn} + bA^{ln} = cA^{mn}$. Then we have

$$a\alpha^{kn} + b\alpha^{ln} = c\alpha^{mn}, \tag{4}$$

$$a\beta^{kn} + b\beta^{ln} = c\beta^{mn}. \tag{5}$$

Dividing (4) by $c\alpha^{mn}$,

$$\frac{a}{c}\alpha^{(k-m)n} + \frac{b}{c}\alpha^{(l-m)n} = 1.$$

Since $a/c \geqslant b/c \geqslant 1$ and $\alpha > 0$, we have

$$\left\lceil \frac{a}{c} \right\rceil \alpha^{(k-m)n} \geqslant \frac{a}{c}\alpha^{(k-m)n}$$

and
$$\left\lceil \frac{a}{c} \right\rceil \alpha^{(l-m)n} \geqslant \frac{b}{c}\alpha^{(l-m)n}.$$
Thus
$$\lceil a/c \rceil \left(\alpha^{(k-m)n} + \alpha^{(l-m)n}\right) \geqslant \frac{a}{c}\alpha^{(k-m)n} + \frac{b}{c}\alpha^{(l-m)n} = 1. \tag{6}$$
Therefore
$$\alpha^{(k-m)n} + \alpha^{(l-m)n} \geqslant \frac{1}{\lceil a/c \rceil}. \tag{7}$$
Since $\alpha \geqslant 1$, we have $0 < \alpha^{-1} \leqslant 1$. Note that both $(k-m)n$ and $(l-m)n$ are negative otherwise
$$\frac{a\alpha^{(k-m)n}}{c} + \frac{b\alpha^{(l-m)n}}{c} > 1.$$
Since $n > N$, we have
$$\log \alpha^n > \log \lceil a/c \rceil + \log 2.$$
Then $\alpha^n > 2\lceil a/c \rceil$. So we have
$$\alpha^{-n} < \frac{1}{2\lceil a/c \rceil}.$$
Since $(k-m)n, (l-m)n \leqslant -1$, we have
$$\alpha^{(k-m)n} + \alpha^{(l-m)n} \leqslant 2\alpha^{-n} < \frac{1}{\lceil a/c \rceil}$$
which contradicts (7). This completes the proof. □

Example 1 Taking $a = b = c = 1$ and
$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$
Then the eigenvalues of A are $(1 \pm \sqrt{5})/2$. By Theorem 1 the equation
$$A^{kn} + A^{ln} = A^{mn}$$
has no solution for $n > 1$, which is due to Grytzuk[5].

Corollary 1 *Let*
$$A = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$
be an integer matrix satisfying the assumptions of Theorem 1. Let a, b, c be positive integers such that $a \geqslant 2c$ and $a \geqslant b \geqslant a - c$. Then for every natural number $n > N$ where
$$N = \frac{2\log 2}{\log \alpha}$$
the equation
$$aA_k^n + bA_l^n = (a-c)A_m^n \tag{8}$$
does not hold.

Proof: Since $a \geqslant 2c$, we have $c/(a-c) \geqslant 1$. Then
$$\left\lceil \frac{a}{a-c} \right\rceil = \left\lceil \frac{a-c+c}{a-c} \right\rceil = \left\lceil 1 + \frac{c}{a-c} \right\rceil = 2.$$
Applying Theorem 1 we show that the equation $aA_k^n + bA_l^n = (a-c)A_m^n$ has no solutions for $n > N$. □

Example 2 Taking $a = 2$, $b = c = 1$ and
$$A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}.$$
Then the eigenvalues of A are $1 \pm \sqrt{2}$. By Corollary 1 the equation
$$2A_k^n + A_l^n = A_m^n \tag{9}$$
has no solution for $n \geqslant 2$.

Next, let F be an algebraic number field and O_F be its ring of integers. Let $k, d \in O_F - \{0\}$. Define
$$F(k,d) = \left\{ \begin{pmatrix} e & f \\ kf & e \end{pmatrix} \,\middle|\, e, f \in O_F, \begin{vmatrix} e & f \\ kf & e \end{vmatrix} = d \right\}.$$
We now consider (3) over the set $F(k,d)$. We first use the following lemma.

Lemma 1 (Ref. 4) *For any positive integer n we have*
$$\begin{pmatrix} e & f \\ kf & e \end{pmatrix}^n = \begin{pmatrix} E_n & F_n \\ kF_n & E_n \end{pmatrix}$$
where
$$E_n = \tfrac{1}{2}(\alpha^n + \beta^n), \quad F_n = \frac{1}{2\sqrt{k}}(\alpha^n - \beta^n),$$
$$\alpha = e + f\sqrt{k}, \quad \beta = e - f\sqrt{k}.$$

We now establish our main theorem on the Fermat-like equation over $F(k,d)$. Our method is based on a proof by Cao and Grytzuk[4].

Theorem 2 *Let a, b, c, d, $k \in O_F \backslash \{0\}$. If $\sqrt{\Delta} \notin F(\sqrt{k})$ where $\Delta = (a^2+b^2-c^2)^2 - 4a^2b^2$ then (3) has no nontrivial solution over $F(k,d)$ for any positive integer n.*

Proof: Suppose on the contrary that (3) has a solution in $F(k,d)$ for some positive integer n. Let
$$X = \begin{pmatrix} e_1 & f_1 \\ kf_1 & e_1 \end{pmatrix}, \quad Y = \begin{pmatrix} e_2 & f_2 \\ kf_2 & e_2 \end{pmatrix},$$
$$Z = \begin{pmatrix} e_3 & f_3 \\ kf_3 & e_3 \end{pmatrix}.$$

By Lemma 1, we have

$$X^n = \begin{pmatrix} E_n^{(1)} & F_n^{(1)} \\ kF_n^{(1)} & E_n^{(1)} \end{pmatrix}, \quad Y^n = \begin{pmatrix} E_n^{(2)} & F_n^{(2)} \\ kF_n^{(2)} & E_n^{(2)} \end{pmatrix},$$

$$Z^n = \begin{pmatrix} E_n^{(3)} & F_n^{(3)} \\ kF_n^{(3)} & E_n^{(3)} \end{pmatrix},$$

where $E_n^{(i)} = \frac{1}{2}(\alpha_i^n + \beta_i^n)$, $F_n^{(i)} = \frac{1}{2\sqrt{k}}(\alpha_i^n - \beta_i^n)$, $\alpha_i = e_i + f_i\sqrt{k}$, and $\beta_i = e_i - f_i\sqrt{k}$. We then have

$$aE_n^{(1)} + bE_n^{(2)} = cE_n^{(3)}, \tag{10}$$

$$aF_n^{(1)} + bF_n^{(2)} = cF_n^{(3)}. \tag{11}$$

From the above equations we have

$$a\alpha_1^n + a\beta_1^n + b\alpha_2^n + b\beta_2^n = c\alpha_3^n + c\beta_3^n, \tag{12}$$

$$a\alpha_1^n - a\beta_1^n + b\alpha_2^n - b\beta_2^n = c\alpha_3^n - c\beta_3^n. \tag{13}$$

From (12) and (13) we have

$$a\alpha_1^n + b\alpha_2^n = c\alpha_3^n, \tag{14}$$

$$a\beta_1^n + b\beta_2^n = c\beta_3^n. \tag{15}$$

From (14) and (15) we obtain

$$a^2\alpha_1^n\beta_1^n + ab\alpha_1^n\beta_2^n + ab\alpha_2^n\beta_1^n + b^2\alpha_2^n\beta_2^n = c^2\alpha_3^n\beta_3^n. \tag{16}$$

Since $\alpha_i\beta_i = d$ we have

$$(a^2 + b^2 - c^2)d^n + ab(\alpha_1^n\beta_2^n + \alpha_2^n\beta_1^n) = 0. \tag{17}$$

Since $d \neq 0$, $\beta_i \neq 0$ for all i. Let $x = (\beta_1/\beta_2)^n$. Note that $x \in F(\sqrt{k})$. Since $\alpha_i = d/\beta_i$ for all i, from (17), we have

$$(a^2 + b^2 - c^n)d^n + ab\left(\left(\frac{d\beta_2}{\beta_1}\right)^n + \left(\frac{d\beta_1}{\beta_2}\right)^n\right) = 0,$$

$$d^n(a^2 + b^2 - c^2) + d^n ab\left(\frac{1}{x} + x\right) = 0.$$

Since $d \neq 0$, we have

$$abx^2 + (a^2 + b^2 - c^2)x + ab = 0.$$

Solving for x, we obtain

$$x = \frac{-(a^2 + b^2 - c^2) \pm \sqrt{(a^2 + b^2 - c^2)^2 - 4a^2b^2}}{2ab}.$$

If $\sqrt{\Delta} = \sqrt{(a^2 + b^2 - c^2)^2 - 4a^2b^2} \notin F(\sqrt{k})$, then $x \notin F(\sqrt{k})$. This is a contradiction. □

Example 3 Taking $a = i + 1$, $b = c = i$, $k \in \mathbb{N}$, $d \in \mathbb{Z} - \{0\}$ and $F = \mathbb{Q}(i)$. Then $\Delta = -4 + 8i$, so $\sqrt{\Delta} \notin \mathbb{Q}(i)$. Thus by Theorem 2 the equation

$$(i + 1)X^n + iY^n = iZ^n,$$

has no solutions over $F(k, d)$ for positive integer n.

Corollary 2 *Let F be a real number field. Let a, b, c, d, $k \in O_F$. If a, b, c, k are positive and $|b - c| < a < b + c$ then the equation*

$$aX^n + bY^n = cZ^n$$

has no solution in X, Y, $Z \in F(k, d)$ for any positive integer n.

Proof: If $|b - c| < a < b + c$ then $\Delta = (a^2 + b^2 - c^2)^2 - 4a^2b^2 < 0$. Thus $\sqrt{\Delta} \notin F(\sqrt{k})$. We then apply Theorem 2 to obtain a result. □

Example 4 Taking $a = b = c = 1$, $k \in \mathbb{N}$, $d \in \mathbb{Z} - \{0\}$ and $F = \mathbb{Q}$. Then $\Delta = -3$. Thus by Theorem 2 the equation $X^n + Y^n = Z^n$ has no solution over $F(k, d)$ for any positive integer n. This result is due to Cao and Grytczuk[4] for $n \geqslant 3$.

Acknowledgements: The author is indebted to a referee for their helpful comments and suggestions. The research is supported by the Centre of Excellence in Mathematics, the Commission on Higher Education, Thailand.

REFERENCES

1. Wiles A (1995) Modular elliptic curves and Fermat's Last theorem. *Ann Math* **141**, 443–551.
2. Domiaty RZ (1966) Solution of $x^4 + y^4 = z^4$ in 2×2 integral matrices. *Amer Math Mon* **73**, 613.
3. Li C, Le M (1995) A note on Fermat's equations in integral 2×2 matrices. *Discuss Math Algebra Stoch Meth* **15**, 135–6.
4. Cao Z, Grytczuk A (1998) Fermat's type equation in the set of 2×2 integral matrices. *Tsukuba J Math* **22**, 637–43.
5. Grytzuk A (1995) On Fermat's equation in the set of integral 2×2 matrices. *Period Math Hung* **30**, 79–84.