KRYSTYNA BIAŁEK AND ALEKSANDER GRYTCZUK

THE EQUATION OF FERMAT IN $G_2(k)$ AND $Q\left(\sqrt{k}\right)$

1. INTRODUCTION

Let $G_2(k)$ be the set of matrices of the form

(1) $$\begin{bmatrix} r & s \\ ks & r \end{bmatrix}$$

where k is fixed integer such that $k \neq 0$ and $r,s \neq 0$ are arbitrary integers.

The purpose of this paper is to give a connection between the solution of Fermat equation in $G_2(k)$ and the solution of this equation in $Q\left(\sqrt{k}\right)$.

Some partial results concerning above problem are given in [1], [2], [4] (comp. [5]).

We prove the following theorems:

THEOREM 1.

The necessary and sufficient condition for the equation

(2) $$A^n + B^n = C^n ,$$

$(n \geq 2)$ to have a solution in elements $A,B,C \in G_2(k)$ is the existence of the numbers $\alpha,\ \beta,\ \gamma \in Q\left(\sqrt{k}\right)$ such that

(3) $$\alpha^n + \beta^n = \gamma^n .$$

THEOREM 2.

Let K be a number field. If $a,b,c \in K$ and

$$a^{2m} + b^{2m} = c^{2m}$$

with m positive integer then

$$A^{4m} + B^{4m} = C^{4m} ,$$

where A,B,C are matrices of the form

$$A = \begin{bmatrix} 0 & 1 \\ a & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 1 \\ c & 0 \end{bmatrix} .$$

2. LEMMAS

In the proofs of the theorems we can use the following lemmas:

LEMMA 1

If

$$\begin{bmatrix} r & s \\ ks & r \end{bmatrix}^n = \begin{bmatrix} R & S \\ kS & R \end{bmatrix}$$

for some $n \geq 2$ then

$$(4) \qquad R = \frac{1}{2} \left[\left(r+s\sqrt{k}\right)^n + \left(r-s\sqrt{k}\right)^n \right] ,$$

and

$$(5) \qquad S = \frac{1}{2\sqrt{k}} \left[\left(r+s\sqrt{k}\right)^n - \left(r-s\sqrt{k}\right)^n \right] .$$

PROOF

In case n=2 the Lemma can be seen directly and one can complete the proof by mathematical induction on n.

LEMMA 2

If

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with integers a,b,c,d, then for every integer $n \geq 2$

$$A^n = \begin{bmatrix} f(a) & b\psi \\ c\psi & f(d) \end{bmatrix},$$

where ψ is an integer,

$$f(a) - f(d) = (a - d)\ \psi$$

and $f(a)$, $f(d)$ are polynomials of degree n.

<u>PROOF</u>

For $n=2$ we have

$$A^2 = \begin{bmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{bmatrix} = \begin{bmatrix} f(a) & b\psi \\ c\psi & f(d) \end{bmatrix} ,$$

where $\psi = a+d$. It is easy to verify that

$$f(a) - f(d) = (a-d)\ (a+d) = (a-d)\ \psi \ .$$

Assume that the Lemma is true for $n=k$, $(k\geq 2)$ that is

$$A^k = \begin{bmatrix} f_1(a) & b\psi_1 \\ c\psi_1 & f_1(d) \end{bmatrix} \quad \text{and} \quad f_1(a) - f_1(d) = (a-d)\psi_1 \ .$$

First we have

$$A^{k+1} = A^k\ A = \begin{bmatrix} f_1(a) & b\psi_1 \\ c\psi_1 & f_1(d) \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} f_2(a) & b\psi_2 \\ c\psi_2^* & f_2(d) \end{bmatrix} ,$$

where

$$\begin{aligned} & f_2(a) = af_1(a) + bc\ \psi_1 \ , \qquad f_2(d) = df_1(d) + bc\ \psi_1 \ , \\ (7) \quad & \\ & \psi_2 = f_1(a) + d\ \psi_1 \ , \qquad \psi_2^* = a\ \psi_1 + f_1(d) \end{aligned}$$

On the other hand

$$(8) \quad A^{k+1} = A\ A^k = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} f_1(a) & b\psi_1 \\ c\psi_1 & f_1(d) \end{bmatrix} =$$

$$= \begin{bmatrix} af_1(a)+ bc\psi_1 & b\left[a\psi_1+f_1(d)\right] \\ c\left[d\psi_1+f_1(a)\right] & df_1(d)+bc\psi_1 \end{bmatrix} .$$

Comparing the entries of A^k A and A A^k we obtain

$$f_1(a) + d\psi_1 = a\psi_1 + f_1(d),$$

hence by (7) we get

$$\psi_2 = \psi_2^*.$$

From (7) it follows that

$$f_2(a) - f_2(d) = af_1(a) - df_1(d)$$

but

$$f_1(a) = f_1(d) + (a-d)\psi_1.$$

Thus

$$f_2(a)-f_2(d)=a\left[f_1(d)+(a-d)\psi_1\right]-df_1(d)=(a-d)\left[f_1(d)+a\psi_1\right].$$

From (7) we have

$$f_1(d) + a\psi_1 = \psi_2^* = \psi_2,$$

thus

$$f_2(a) - f_2(d) = (a-d)\psi_2$$

what ends the proof.

LEMMA 3.

If a matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with $n\geq 2$ and integers a,b,c,d satisfies

$$A^n = \begin{bmatrix} R & S \\ kS & R \end{bmatrix},$$

where k is fixed integer such that $k\neq 0$ and $R,S\neq 0$ are integers, then

$$A \in G_2(k).$$

PROOF

From the assumption we have

$$(9)\qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix}^n = \begin{bmatrix} R & S \\ kS & R \end{bmatrix},$$

for some $n\geq 2$ and $S\neq 0$.

By Lemma 2 we have

$$(10)\qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix}^n = \begin{bmatrix} f_1(a) & b\psi_1 \\ c\psi_1 & f_1(d) \end{bmatrix},$$

where

$$f_1(a) - f_1(d) = (a-d)\psi_1.$$

From (9) and (10) we obtain

$$\begin{bmatrix} f_1(a) & b\psi_1 \\ c\psi_1 & f_1(d) \end{bmatrix} = \begin{bmatrix} R & S \\ kS & R \end{bmatrix}.$$

Thus

$$f_1(a) = f_1(d) = R, \quad c\psi_1 = kS, \quad b\psi_1 = S.$$

From this we have

$$f_1(a) - f_1(d) = 0.$$

Since $S\neq 0$, then we obtain

$$\psi_1\neq 0 \quad \text{and} \quad c\psi_1 = kb\psi_1$$

hence

$$c = kb.$$

On the other hand

$$(a-d)\psi_1 = f_1(a) - f_1(d) = 0.$$

By the fact that $\psi_1\neq 0$ we get $a=d$ and the proof is complete.

3. PROOFS OF THE THEOREMS.

PROOF OF THEOREM 1.

Assume that $A,B,C \in G_2(k)$ and let

$$A = \begin{bmatrix} r_1 & s_1 \\ ks_1 & r_1 \end{bmatrix}, \quad B = \begin{bmatrix} r_2 & s_2 \\ ks_2 & r_2 \end{bmatrix}, \quad C = \begin{bmatrix} r_3 & s_3 \\ ks_3 & r_3 \end{bmatrix}$$

such that

$$(11) \qquad A^n + B^n = C^n.$$

By Lemma 1 we obtain

$$A^n = \begin{bmatrix} M_1 & N_1 \\ kN_1 & M_1 \end{bmatrix}, \quad B^n = \begin{bmatrix} M_2 & N_2 \\ kN_2 & M_2 \end{bmatrix}, \quad C^n = \begin{bmatrix} M_3 & N_3 \\ kN_3 & M_3 \end{bmatrix},$$

where

$$(12) \qquad \begin{aligned} M_m &= \frac{1}{2}\left[\left(r_m+s_m\sqrt{k}\right)^n+\left(r_m-s_m\sqrt{k}\right)^n\right], \\ N_m &= \frac{1}{2\sqrt{k}}\left[\left(r_m+s_m\sqrt{k}\right)^n-\left(r_m-s_m\sqrt{k}\right)^n\right], \quad m=1,2,3. \end{aligned}$$

Hence by (11) we have

$$(13) \qquad \begin{aligned} M_3 &= M_1 + M_2 \\ N_3 &= N_1 + N_2. \end{aligned}$$

From (12) and (13) we get

$$\left(r_1+s_1\sqrt{k}\right)^n+\left(r_2+s_2\sqrt{k}\right)^n = \left(r_3+s_3\sqrt{k}\right)^n.$$

Putting in the last equality

$$\alpha = r_1+s_1\sqrt{k}, \quad \beta = r_2+s_2\sqrt{k}, \quad \gamma = r_3+s_3\sqrt{k},$$

we obtain

$$\alpha^n + \beta^n = \gamma^n,$$

where $\alpha,\beta,\gamma \in Q\left(\sqrt{k}\right)$. Now, let $\alpha,\beta,\gamma \in Q\left(\sqrt{k}\right)$. Then we can write

$$\alpha = r_1+s_1\sqrt{k}, \quad \beta = r_2+s_2\sqrt{k}, \quad \gamma = r_3+s_3\sqrt{k}$$

and

$$\bar{\alpha} = r_1-s_1\sqrt{k}, \quad \bar{\beta} = r_2-s_2\sqrt{k}, \quad \bar{\gamma} = r_3-s_3\sqrt{k},$$

with integers r_m, s_m, $m=1,2,3$.
From the assumption we have

$$\alpha^n+\beta^n=\gamma^n.$$

It is easy to see that

$$(\bar{\alpha})^n+(\bar{\beta})^n=(\bar{\gamma})^n.$$

Thus we obtain

$$(14) \qquad \frac{1}{2}\left(\alpha^n+\bar{\alpha}^n\right)+\frac{1}{2}\left(\beta^n+\bar{\beta}^n\right)=\frac{1}{2}\left(\gamma^n+\bar{\gamma}^n\right),$$

and

$$(15) \qquad \frac{1}{2\sqrt{k}}\left(\alpha^n-\bar{\alpha}^n\right)+\frac{1}{2\sqrt{k}}\left(\beta^n-\bar{\beta}^n\right)=\frac{1}{2\sqrt{k}}\left(\gamma^n-\bar{\gamma}^n\right).$$

Donote

$$(16) \qquad M_1=\frac{1}{2}\left(\alpha^n+\bar{\alpha}^n\right), M_2=\frac{1}{2}\left(\beta^n+\bar{\beta}^n\right), M_3=\frac{1}{2}\left(\gamma^n+\bar{\gamma}^n\right).$$

$$(17) \qquad N_1=\frac{1}{2\sqrt{k}}\left(\alpha^n-\bar{\alpha}^n\right), N_2=\frac{1}{2\sqrt{k}}\left(\beta^n-\bar{\beta}^n\right), N_3=\frac{1}{2\sqrt{k}}\left(\gamma^n-\bar{\gamma}^n\right).$$

From this and from (14),(15) we have

$$(18) \qquad M_3 = M_1 + M_2, \qquad N_3 = N_1 + N_2 .$$

Consider the matrices A_1, B_1, C_1 of the form

$$A_1=\begin{bmatrix} M_1 & N_1 \\ kN_1 & M_1 \end{bmatrix}, \quad B_1=\begin{bmatrix} M_2 & N_2 \\ kN_2 & M_2 \end{bmatrix}, \quad C_1=\begin{bmatrix} M_3 & N_3 \\ kN_3 & M_3 \end{bmatrix},$$

where $N_m \neq 0$, $m=1,2,3$.

By (18) we have

$$A_1 + B_1 = C_1.$$

From the above equality and from Lemma 1 and Lemma 3 we obtain that there exist the matrices A,B,C such that

$$A_1 = A^n, \quad B_1 = B^n, \quad C_1 = C^n$$

and therefore we have

$$A^n + B^n = C^n.$$

Thus A,B,C are matrices of the form

$$A = \begin{bmatrix} r_1 & s_1 \\ ks_1 & r_1 \end{bmatrix}, \quad B = \begin{bmatrix} r_2 & s_2 \\ ks_2 & r_2 \end{bmatrix}, \quad C = \begin{bmatrix} r_3 & s_3 \\ ks_3 & r_3 \end{bmatrix}$$

hence $A,B,C \in G_2(k)$, what gives the proof of the Theorem.

PROOF OF THEOREM 2.

Let

$$(19) \qquad A = \begin{bmatrix} r & s \\ as & r \end{bmatrix}$$

then by Lemma 1 we have

$$(20) \qquad \begin{bmatrix} r & s \\ as & r \end{bmatrix}^n = \begin{bmatrix} R & S \\ aS & R \end{bmatrix},$$

where

$$R = \frac{1}{2}\left[\left(r+s\sqrt{a}\right)^n+\left(r-s\sqrt{a}\right)^n\right],$$

(21)

$$S = \frac{1}{2\sqrt{a}}\left[\left(r+s\sqrt{a}\right)^n-\left(r-s\sqrt{a}\right)^n\right].$$

Putting in (21) r=0, s=1 we get

$$R = \frac{1}{2}\left[\left(\sqrt{a}\right)^n+\left(-\sqrt{a}\right)^n\right],$$

$$S = \frac{1}{2\sqrt{a}} \left[\left(\sqrt{a}\right)^n - \left(-\sqrt{a}\right)^n\right].$$

For n=2k

(22) $\quad R = a^{\frac{n}{2}}$ and $S=0$.

follows. By (20) and (22) we get

$$A^n = \begin{bmatrix} 0 & 1 \\ a & 0 \end{bmatrix}^n = \begin{bmatrix} a^{\frac{n}{2}} & 0 \\ 0 & a^{\frac{n}{2}} \end{bmatrix} = a^{\frac{n}{2}} . \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Similarly we obtain

$$B^n = b^{\frac{n}{2}} . \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad C^n = c^{\frac{n}{2}} . \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

For n=4m we have

$$A^{4m}+B^{4m}=a^{2m} . \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b^{2m} . \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} =$$

$$= \left(a^{2m}+b^{2m}\right) . \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = c^{2m} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = C^{4m}$$

and the proof is complete.

From Theorem 2 we get the following Corollary:

<u>COROLLARY</u> (R. Z. Domiaty [3])

If $K=Q$ and $a,b,c \in Z$ then the equation

$$A_a^4 + B_b^4 = C_c^4$$

have infinitely solutions of the form

$$A_a = \begin{bmatrix} 0 & 1 \\ a & 0 \end{bmatrix}, \ B_b = \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix}, \ C_c = \begin{bmatrix} 0 & 1 \\ c & 0 \end{bmatrix},$$

where

$a=\left(m^2-n^2\right).l$, $\quad b=2mnl$, $\quad c=\left(m^2+n^2\right).l$, $\quad m>n$, $\quad (m,n)=1$, $\quad l\geq 1$.

REFERENCES

[1] E.D.Bolker - "Solutions of $A^k+B^k=C^k$ in n×n integral matrices" - Amer. Math. Monthly,75,1968,759-760.

[2] J.I.Brenner and J.de Pillis - "Fermat's equation $A^p B^p =C^p$ for matrices of integers" - Math. Mag.,45,1972,12-15.

[3] R.Z.Domiaty - "Solutions of $x^4+y^4=z^4$ in 2×2 integral matrices" - Amer. Math. Monthly,73,1966,631.

[4] R.Z.Domiaty - "Lösungen der Gleichung $x^n+y^n=z^n$ mit $n=2^m$ im Ring gewisser ganzzahliger Matrizen" - Elem. Math.21,1966,5-7.

[5] P.Ribenboim - "13 lectures on Fermat's last theorem" Springer-Verlag; New York-Heidelberg-Berlin,1980.