Discussiones Mathematicae
General Algebra and Applications 20 (2000) 193–198

SOME CLASSES OF DIOPHANTINE EQUATIONS CONNECTED WITH McFARLAND'S AND MA'S CONJECTURES

Zhenfu Cao [1]
Department of Mathematics, Harbin Institute of Technology
Harbin 150001, P. R. China
e-mail: zfcao@hope.hit.edu.cn

and

Aleksander Grytczuk
Institute of Mathematics, Kotarbiński Pedagogical University
pl. Słowiański 6, 65–069 Zielona Góra, Poland
e-mail: agryt@lord.wsp.zgora.pl

Abstract

In this paper we consider some special classes of Diophantine equations connected with McFarland's and Ma's conjectures about difference sets in abelian groups and we obtain an extension of known results.

Keywords: difference sets, diophantine equations, Pell's equations.

1991 Mathematics Subject Classification: 11D09, 05B10.

1. Introduction

Let G be finite multiplicative group of order v. A k-subset D of G is called a $(v,\, k,\, \lambda)$-*difference* set in G if and only if the "differences" $d_1 d_2^{-1}$ for $d_1,\, d_2 \in D$ with $d_1 \neq d_2$, give every nonidentity element of G precisely λ times. If G is abelian, then D is called an *abelian difference set.*

[1]Supported by National Natural Science Foundation of China and Heilongjiang Province Natural Science Foundation.

An important concept in the theory of difference sets is the concept of *multipliers*. A multiplier is an integer t such that $\{d^t : d \in D\} = Dg$ for some "translate" Dg of D.

One of the unsolved problems concerning difference sets with -1 as a multiplier is McFarland's conjecture (see, K.T. Arasu [1]):

Conjecture 1. *If a nontrivial $(v,\, k,\, \lambda)$-difference set exists in an abelian group with -1 as a multiplier, then either $v = 4n$, where $n = k - \lambda = 625$ or $v = 4000$.*

S.L. Ma [8] posed the following two number-theoretic conjectures that would imply Conjecture 1:

Conjecture 2. *Let p be an odd prime and $a,\, b,\, t, r \in \boldsymbol{N}$. Then*

$$\text{(A)} \qquad Y = 2^{2a}p^{2t} - 2^{2a}p^{t+r} + 1 \textit{ is a square if and only if } t = r;$$

$$\text{(B)} \qquad Z = 2^{2b+2}p^{2t} - 2^{b+2}p^{t+r} + 1 \textit{ is a sqare}$$

$$\textit{if and only if } p = 5,\ b = 3,\ t = 1,\ r = 2.$$

In the paper [8], Ma also obtained some partial results concerning Conjecture 2, namely:

Result 1. *If Y in (A) is square, then $r \le t < 2r$.*

Result 2. *If Z in (B) is square, then $t < r$.*

In 1994 the first author claimed (see [2]) that the Conjecture 2 holds.

Recently, Yongdong Guo in the paper [7] gave a generalization of Result 1, proving that if $k > 1$ is odd and $r < t < 2r$, then the exponential Diophantine equation:

$$\text{(1)} \qquad x^2 = 2^{2a}k^{2t} - 2^{2a}k^{t+r} + 1, \ \text{ where } \ x,\, a,\, k,\, t,\, r \in \boldsymbol{N}$$

has no solution.

Let

$$x,\, y,\, a,\, b,\, k_i,\, t_i,\, r_i \in \boldsymbol{N}, \quad i = 1, 2, \ldots, s, \quad \text{and } \delta \in \{-1, 1\}.$$

In the present paper we consider the following Diophantine equations:

$$x^2 = 2^{2a} k_1^{2t_1} \dots k_s^{2t_s} y^2 - 2^{a+b} k_1^{t_1+r_1} \dots k_s^{t_s+r_s} \delta + 1; \tag{2}$$

$$x^2 = k_1^{2t_1} \dots k_s^{2t_s} y^2 - 2^e k_1^{t_1+r_1} \dots k_s^{t_s+r_s} \delta + 2, \quad \text{where } e \in \{0,1\}; \tag{3}$$

and

$$x^2 = k_1^{2t_1} \dots k_s^{2t_s} y^2 - 4 k_1^{t_1+r_1} \dots k_s^{t_s+r_s} \delta + 4. \tag{4}$$

We prove the following results:

Theorem 1. *Consider equation (2) with $t_i > r_i$ for $i = 1, 2, \dots, s$, $a > b$, and add y. Then Diophantine equation (2) has only solution given by formulas:*

$$x = 2^{a+b-1} k_1^{t_1+r_1} \dots k_s^{t_s+r_s} - \delta \quad \text{and} \quad y = 2^{b-1} k_1^{r_1} \dots k_s^{r_s}.$$

If $a = b$ and y odd, then Diophantine equation (2) has only solution given by formulas:

$$x = 2k_1^{t_1+r_1} ... k_s^{t_s+r_s} - \delta, \quad y = k_1^{r_1} ... k_s^{r_s} \quad \text{and} \quad 2 \nmid k_1 ... k_s.$$

From the Theorem 1 follows the following:

Corollary. If $t > r$, then Diophantine equation (1) has no solution.

Theorem 2. *If $t_i > r_i$ for $i = 1, 2, \dots, s$, then Diophantine equation (3) has no solution.*

Theorem 3. *If $t_i > r_i$ for $i = 1, 2, \dots, s$, then Diophantine equation (4) has only solution given by formulas*

$$x = k_1^{t_1+r_1} \dots k_s^{t_s+r_s} - 2\delta \quad \text{and} \quad y = k_1^{r_1} \dots k_s^{r_s}.$$

Moreover, we can also prove similar results on the following Diophantine equations:

$$x^2 = 2^{2a} k_1^{2t_1} \dots k_s^{2t_s} y^2 - 2^{a+b} k_1^{t_1+r_1} \dots k_s^{t_s+r_s} \delta - 1, \tag{5}$$

$$x^2 = k_1^{2t_1} \dots k_s^{2t_s} y^2 - 2^e k_1^{t_1+r_1} \dots k_s^{t_s+r_s} \delta - 2, \tag{6}$$

$$x^2 = k_1^{2t_1} \dots k_s^{2t_s} y^2 - 4 k_1^{t_1+r_1} \dots k_s^{t_s+r_s} \delta - 4, \tag{7}$$

with the corresponding restrictions as in (2), (3) and (4).

2. Basic Lemmas

Let $D \in \boldsymbol{N}$ be a non-square and let $y|^*D$ denote that D is divided exactly by each prime factor of y.

Lemma 1 ([3], p. 154–155, cf. [9]). *If $x_1, y_1 \in \boldsymbol{N}$, $x_1^2 - Dy_1^2 = 1$ and $x_1 > \frac{1}{2}y_1^2 - 1$, then $x_1 + y_1\sqrt{D}$ is the fundamental solution of the Pell's equation*

$$x^2 - Dy^2 = 1. \tag{8}$$

If $x_1, y_1 \in \boldsymbol{N}$, $x_1^2 - Dy_1^2 = 4$ and $x_1^2 > y_1^2 - 2$, then $x_1 + y_1\sqrt{D}$ is the fundamental solution of the Diophantine equation

$$x^2 - Dy^2 = 4. \tag{9}$$

■

Lemma 2 ([11]). *If $x_1, y_1 \in \boldsymbol{N}$, $x_1^2 - Dy_1^2 = 1$ and $y_1|^*D$, then $x_1 + y_1\sqrt{D}$ is the fundamental solution of the Pell's equation* (8). ■

Lemma 3 ([4]). *Let $a, b, x_1, y_1 \in \boldsymbol{N}$, $a \neq 2$ and $ax_1^2 - by_1^2 = 2$, $D = ab$. If $a = 1$, $y_1|^*b$, then $\frac{1}{2}\left(x_1^2 + by_1^2\right) + x_1y_1\sqrt{b}$ is the fundamental solution of the Pell's equation* (8).

If $x_1|^*a$ or $y_1|^*b$, then $\frac{1}{2}\left(ax_1^2 + by_1^2\right) + x_1y_1\sqrt{ab} = \varepsilon$ or is equal to ε^3, where ε is the fundamental solution of the Pell's equation (8). ■

Lemma 4 ([5]). *Let $a, b, x_1, y_1 \in \boldsymbol{N}$, $a \neq 4$ and $ax_1^2 - by_1^2 = 4$, $D = ab$. If $a = 1$, $y_1|^*b$, then $x_1 + y_1\sqrt{b}$ is the fundamental solution of equation* (9).

If $x_1|^*a$ or $y_1|^*b$, then $\frac{1}{2}\left(ax_1^2 + by_1^2\right) + x_1y_1\sqrt{ab} = \omega$ or is equal to $\frac{1}{4}\omega^3$, except when $a = 5$, $b = 1$, $x_1 = 5$, $y_1 = 11$, where ω is the fundamental solution of equation (9). ■

From Lemma 1 one can deduce the following:

Lemma 5 (see also [6] and [10]). *Let ε be the fundamental solution of Pell's equation* (8). *If $D = s\left(st^2 - \delta\right)$, with $s, t \in \boldsymbol{N}$, and $s > 1$, then $\varepsilon = 2st^2 - \delta + 2t\sqrt{D}$.*

If $D = s\left(st^2 - 2\delta\right) > 0$, with $s, t \in \boldsymbol{N}$, and $\delta \in \{-1, 1\}$, then $\varepsilon = st^2 - \delta + t\sqrt{D}$.

If $D = s\left(st^2 - 4\delta\right) > 0$, with $s, t \in \boldsymbol{N}$, then $st^2 - 2\delta + t\sqrt{D}$ is the fundamental solution of equation (9). ■

3. Proof of Theorems

***Proof of Theorem* 1.** From (2) we have

$$(10)\quad x^2=2^{a-b}k_1^{t_1-r_1}\dots k_s^{t_s-r_s}\left(2^{a-b}k_1^{t_1-r_1}\dots k_s^{t_s-r_s}y^2-\delta\right)\left(2^b k_1^{r_1}\dots k_s^{r_s}\right)^2+1.$$

Putting in (10) $X=x$, $t=y$, $s=2^{a-b}k_1^{t_1-r_1}\dots k_s^{t_s-r_s}$ and $Y=2^b k_1^{r_1}\dots k_s^{r_s}$ we obtain

$$(11)\qquad X^2-s\left(st^2-\delta\right)Y^2=1.$$

By Lemma 5, it follows that the fundamental solution of the Pell's equation: $U^2-s\left(st^2-\delta\right)V^2=1$ is given by $\varepsilon=2st^2-\delta+2t\sqrt{s\left(st^2-\delta\right)}$.

On the other hand we have $Y|^{*}s\left(st^2-\delta\right)$, therefore from Lemma 2 and (11), we obtain $X+Y\sqrt{s\left(st^2-\delta\right)}=2st^2-\delta+2t\sqrt{s\left(st^2-\delta\right)}$, so $X=2st^2-\delta$ and $Y=2t$.

The proof of the Theorem 1 is complete. ■

***Proof of Theorem* 2.** From (3) we obtain

$$(12)\quad x^2=k_1^{t_1-r_1}\dots k_s^{t_s-r_s}\left(k_1^{t_1-r_1}\dots k_s^{t_s-r_s}y^2-2^e\delta\right)\left(k_1^{r_1}\dots k_s^{r_s}\right)^2+2.$$

Applying Lemma 3 to (12), we get

$$(13)\quad \varepsilon=\frac{1}{2}\left(x^2+k_1^{t_1-r_1}\dots k_s^{t_s-r_s}\left(k_1^{t_1-r_1}\dots k_s^{t_s-r_s}y^2-2^e\delta\right)\left(k_1^{r_1}\dots k_s^{r_s}\right)^2\right)+ \\ +xk_1^{r_1}\dots k_s^{r_s}\sqrt{D},$$

where ε is the fundamental solution of Pell's equation (8) and

$$D=k_1^{t_1-r_1}\dots k_s^{t_s-r_s}\left(k_1^{t_1-r_1}\dots k_s^{t_s-r_s}y^2-2^e\delta\right).$$

Hence, by Lemma 5 it follows that

$$\varepsilon=\begin{cases} 2k_1^{t_1-r_1}\dots k_s^{t_s-r_s}y^2-\delta+2y\sqrt{D}, & if\ \ e=0\\ k_1^{t_1-r_1}\dots k_s^{t_s-r_s}y^2-\delta+y\sqrt{D}, & if\ \ e=1\end{cases},$$

and consequently, we see that (13) is impossible. The proof of the Theorem 2 is complete. ■

Remark. The proof of the Theorem 3 is completely similar to the proof of the Theorem 1.

References

[1] K.T. Arasu, *Recent results on difference sets*, p. 1–23 in: "*Coding Theory and Design Theory*", Part II, Springer-Verlag, Berlin-New York 1990.

[2] Z. Cao, *Some Diophantine equations in difference sets*, a lecture in: "*5-th National Combinatorial Mathematics Conference*", Shanghai 1994.

[3] Z. Cao, "*Introduction to Diophantine equations*" (Chinese), Harbin Inst. of Technology Press, Harbin 1989.

[4] Z. Cao, *On the equation* $ax^m - by^n = 2$, Chinese Sci. Bull. **35** (1990), 1227–1228.

[5] Z. Cao, *On the Diophantine equation* $\frac{ax^m-4c}{abx-4c} = by^2$ (Chinese), J. Harbin Inst. Tech. **23** (1991), suppl., 110–112.

[6] G. Degert, *Über die Bestimung der Grundeinheit gewisser reell-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 92–97.

[7] Y.-D. Guo, *On the exponential Diophantine equation* $x^2 = 2^{2a}k^{2m} - 2^{2a}k^{m+n} + 1$, Discuss. Math.- Algebra & Stochastic Methods **16** (1996), 57–60.

[8] S.L. Ma, *McFarland's conjecture on abelian difference sets with multiplier* -1, Des. Codes Cryptogr. **1** (1992), 321–332.

[9] L.J. Mordell, "*Diophantine Eqations*", Academic Press, London 1969.

[10] C. Richaud, *Sur la résolution des équations* $x^2 - Ay^2 = \pm$, Atti Acad. Pontif. Nuovi Lincei, 1866, 177–182.

[11] C. Størmer, *Quelques theorems sur l'equation de Pell* $x^2 - Dy^2 = \pm 1$ *et leur applications*, Skr. Norske Vid. Acad., I Selsk. Mat. Natur. Kl., No. **2** (1897), 48 pp.

Received 11 March 1998
Revised 24 October 2000
Revised 4 December 2000