DIOPHANTINE TRIPLES AND EXTENDIBILITY OF $\{1,2,5\}$ AND $\{1,5,10\}$

YIFAN ZHANG AND GEORGE GROSSMAN

Abstract. In this paper we consider Diophantine triples, (denoted $D(n)$-3-tuples,) $\{1,2,5\}$, $\{1,5,10\}$ for the case $n=-1$. We show using properties of Lucas and Fibonacci numbers that neither of 3-tuples $\{1,2,5\}$, $\{1,5,10\}$ can be extended to a $D(-1)$-4-tuple.

1. INTRODUCTION

Definition 1.1. *A set of m positive integers is called a Diophantine m-tuple with the property $D(n)$ or simply $D(n)$-m-tuple, if the product of any two elements of this set increased by n is a perfect square.*

As a special case, a Diophantine m-tuple is a set of m positive integers with the property: the product of any two of them increased by one unit is a perfect square, for example, $\{1, 3, 8, 120\}$ is a Diophantine quadruple, since we have

$$1\times 3+1=2^2, 1\times 8+1=3^2, 1\times 120+1=11^2,$$

$$3\times 8+1=5^2, 3\times 120+1=19^2, 8\times 120+1=31^2.$$

The study of Diophantine m-tuple can be traced back to the third century AD, when the Greek mathematician Diophantus discovered that $\left\{\frac{1}{16},\frac{33}{16},\frac{17}{4},\frac{105}{16}\right\}$ is a set of four rationals which has the above property. Then Fermat obtained the first Diophantine quadruple $\{1, 3, 8, 120\}$. Astoundingly, $\frac{777480}{8288641}$ was found to extend the Fermat's set to $\left\{1,3,8,120,\frac{777480}{8288641}\right\}$ and then the product of any two elements of this set increased by one unit is a perfect square of a rational number, which was Euler's contribution. Moreover, he acquired the infinite family of Diophantine quadruple $\{a,b,a+b+2r,4r\,(r+a)\,(r+b)\}$, if $ab+1=r^2$. In January 1999, Gibbs [8] found the first set of six positive rationals with the above property. In the integer case, there is a famous conjecture: there does not exist a Diophantine quintuple.

The case $n\neq 1$ also have been studied by several mathematicians, for example, $\{1,2,5\}$ is a $D(-1)$-triple. It is interesting to note that if n is an integer of form $n=4k+2$, then there does not exist a Diophantine quadruple with the property $D(n)$. This theorem has been independently proved by Brown [2], Gupta & Singh [9] and Mohanty & Ramasamy [13] all in 1985. In 1993, Dujella [3] proved that if an integer n does not have the form $n=4k+2$ and $n\notin S=\{-4,-3,-1,3,5,8,12,20\}$, then there exists at least one Diophantine quadruple with the property $D(n)$. In the case $n=-1$, the conjecture—there does not exist a $D(-1)$-quadruple is known as $D(-1)$-quadruple conjecture.

In 1985, Brown [2] proved the nonextendability of the Diophantine $D(-1)$ triple $\{1,2,5\}$. Walsh [15] and Kihel [10] also independently proved that in 1999 and 2000 respectively. In 1984, Mohanty & Ramasamy [12] proved that the Diophantine $D(-1)$ triple $\{1,5,10\}$ can not be extended to a $D\,(-1)$ quadruple. Furthermore, Brown [2] proved that the following triple

$$\left\{n^2+1,(n+1)^2+1,(2n+1)^2+4\right\},$$

can not be extended to a Diophantine quadruple with the property $D(-1)$ if $n \equiv 0 \pmod 4$. $\{17, 26, 85\}$ is an example when $n = 4$. Dujella [4] was the first mathematician who proved the nonextendability for all triples of the form $\{1, 2, c\}$ in 1998. The endeavor in proving that $\{1, 5, c\}$ can not be extended was mostly attributed to Muriefah & Al-Rashed [14]. In 2005, Filipin [7] proved the nonextendability of $\{1, 10, c\}$.

In [2, 4, 7, 10, 12, 14, 15] solution techniques involved the intersection of solutions of systems of certain Pellian equations, including also employing methods such as linear forms in logarithms from the results of Baker and Davenport, [1], and other deep theoretical results from Diophantine analysis. Our paper uses only elementary number theory including use of results related to Legendre symbols, basic properties of Fibonacci and Lucas numbers with congruences, and thus, represents a distinctly original approach, i.e., without use of Pellian equations.

There does not exist a Diophantine quintuple with the property $D(-1)$. This was proved by Dujella & Fuchs [6] in 2005. Moreover, in 2007, Dujella, Filipin & Fuchs [5] proved that there are only exist finitely many quadruples with the property $D(-1)$.

2. NONEXTENDABILITY OF $\{1, 2, 5\}$

We will use the property of Fibonacci and Lucas sequences to prove the nonextendability of Diophantine triple $\{1, 2, 5\}$ with the property $D(-1)$.

Definition 2.1. *F_n is Fibonacci sequence beginning with $F_0 = 0$, $F_1 = 1$ and satisfying the property $F_{n+2} = F_{n+1} + F_n$. L_n is Lucas sequence beginning with $L_0 = 2$, $L_1 = 1$ and satisfying the property $L_{n+2} = L_{n+1} + L_n$.*

It is well-known that if (X, Y) are positive integers such that $X^2 - 5Y^2 = \pm 4$, then $(X, Y) = (L_m, F_m)$ for some positive integer m and the sign on the right is given by $(-1)^m$, also this result can be found in Koshy's [11] book, Theorem 5.4 in page 75 and Theorem 5.10 in page 83. If $1, 5, d$ are in the same $D(-1)$ set, then exists integers A, B such that $d - 1 = A^2$ and $5d - 1 = B^2$, thus we have $B^2 - 5A^2 = 4$ and then $A = F_{2n}$ for some positive integer n.

In order to prove that $\{1, 2, 5, d\}$ and $\{1, 5, 10, d\}$ are not Diophantine quadruple, we need prove $2d - 1$ and $10d - 1$ are not perfect squares, respectively. Since $d = A^2 + 1$ and $A = F_{2n}$ for some positive integer n, we reduce these two questions to prove $2F_{2n}^2 + 1$ and $10F_{2n}^2 + 9$ are not perfect squares for any positive integer n, respectively.

Lemma 2.2. *For any nonnegative integer q,*
$$5\left(F_{3^q}^2 + 2F_{2\cdot 3^q}^2 + 1\right) = \left(L_{2\cdot 3^q} + 1\right)\left(2L_{2\cdot 3^q} - 1\right).$$

Proof. This lemma can be derived by the following calculation:
$$\begin{aligned}
&5\left(F_{3^q}^2 + 2F_{2\cdot 3^q}^2 + 1\right) - \left(L_{2\cdot 3^q} + 1\right)\left(2L_{2\cdot 3^q} - 1\right)\\
&= 5F_{3^q}^2 + 10F_{2\cdot 3^q}^2 + 5 - 2L_{2\cdot 3^q}^2 - L_{2\cdot 3^q} + 1\\
&= \left(5F_{3^q}^2 - 4\right) + 2\left(5F_{2\cdot 3^q}^2 + 4\right) + 2 - 2L_{2\cdot 3^q}^2 - L_{2\cdot 3^q}\\
&= L_{3^q}^2 + 2 - L_{2\cdot 3^q}\\
&= L_{2\cdot 3^q} - L_{2\cdot 3^q}\\
&= 0.
\end{aligned}$$
□

We will use this formula for Lemma 2.3 and Lemma 3.1, $F_{nm}^2 - F_m^2 = F_{(n+1)m}F_{(n-1)m}$ with $m(n-1)$ even, this formula can be found in Koshy's [11] book, the 55th Fibonacci and Lucas identity in page 90 with n replaced by m and $2k$ replaced by $m(n-1)$. Let $\alpha = \frac{\sqrt{5}+1}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$, then $F_m = \frac{1}{\sqrt{5}}(\alpha^m - \beta^m)$, $L_m = \alpha^m + \beta^m$ and $\alpha\beta = -1$.

Lemma 2.3. *If n is a positive integer not divisible by 3, then $F^2_{2\cdot 3^q\cdot n} \equiv F^2_{2\cdot 3^q} \pmod{(L_{2\cdot 3^q}+1)}$.*

Proof. If $3 \nmid n$, then $3 \mid (n+1)$ or $3 \mid (n-1)$, thus $F_{3m} \mid F_{(n+1)m}$ or $F_{3m} \mid F_{(n-1)m}$. For even integer m, $F_{3m} = \frac{1}{\sqrt{5}}\left(\alpha^{3m}-\beta^{3m}\right) = \frac{1}{\sqrt{5}}\left(\alpha^m-\beta^m\right)\left(\alpha^{2m}+\alpha^m\beta^m+\beta^{2m}\right)$
$= \frac{1}{\sqrt{5}}\left(\alpha^m-\beta^m\right)\left(\left(\alpha^m+\beta^m\right)^2-(\alpha\beta)^m\right) = F_m\left(L_m^2-1\right) = F_m\left(L_m+1\right)\left(L_m-1\right)$, then $(L_m+1) \mid F_{3m} \mid \left(F^2_{nm}-F^2_m\right)$. By letting $m = 2\cdot 3^q$, we get $F^2_{2\cdot 3^q\cdot n} \equiv F^2_{2\cdot 3^q} \pmod{(L_{2\cdot 3^q}+1)}$. $\square$

$\{L_m\}_{m\geq 1}$ is periodic modulo 4 with period 6, then $L_{2\cdot 3^q} \equiv L_0 = 2 \pmod 4$ for $q \geq 1$.

Theorem 2.4. *The Diophantine triple $\{1,2,5\}$ cannot be extended to a Diophantine quadruple $\{1,2,5,d\}$ with the property $D(-1)$, for all integers $d > 5$.*

Proof. We only need to prove $2F^2_{2n}+1$ is not a perfect square for any positive integer n. Suppose there exists a positive integer l such that $l^2 = 2F^2_{2n}+1$. Write $2n$ in the form $2n = 2\cdot 3^q\cdot k$ with $q \geq 0$ and $3 \nmid k$.

If $q = 0$, then $F^2_{2n} = F^2_{2\cdot 3^0\cdot k} \equiv F^2_{2\cdot 3^0} = F^2_2 = 1 \pmod{(L_{2\cdot 3^0}+1)}$, then $F^2_{2n} \equiv 1 \pmod 4$ and $l^2 = 2F^2_{2n}+1 \equiv 3 \pmod 4$, a contradiction to the fact that the square of any integer is congruent to 0 or 1 modulo 4.

If $q \geq 1$, then $L_{2\cdot 3^q} \equiv 2 \pmod 4$, then $L_{2\cdot 3^q}+1 \equiv 3 \pmod 4$. Therefore, there is a prime number p such that $p \mid (L_{2\cdot 3^q}+1)$ and $p \equiv 3 \pmod 4$.

According to Lemma 2.2, $p \mid \left(5\left(F^2_{3^q}+2F^2_{2\cdot 3^q}+1\right)\right)$, since $p \nmid 5$, then $2F^2_{2\cdot 3^q}+1 \equiv -F^2_{3^q} \pmod p$. Then we have $1 = \left(\frac{l^2}{p}\right) = \left(\frac{2F^2_{2n}+1}{p}\right) = \left(\frac{2F^2_{2\cdot 3^q\cdot k}+1}{p}\right) = \left(\frac{2F^2_{2\cdot 3^q}+1}{p}\right) = \left(\frac{-F^2_{3^q}}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{F^2_{3^q}}{p}\right) = \left(\frac{-1}{p}\right) = -1$ since $p \equiv 3 \pmod 4$, a contradiction.

In conclusion, the Diophantine triple $\{1,2,5\}$ cannot be extended to a Diophantine quadruple $\{1,2,5,d\}$, for all integers $d > 5$. $\square$

3. NONEXTENDABILITY OF $\{1,5,10\}$

Lemma 3.1. *If q and n are positive integers and n is odd, then $F^2_{2^q\cdot n} \equiv F^2_{2^q} \pmod{L_{2^{q+1}}}$.*

Proof. In formula $F^2_{nm}-F^2_m = F_{(n+1)m}F_{(n-1)m}$, if n is odd, then $4 \mid (n+1)$ or $4 \mid (n-1)$, thus $F_{4m} \mid F_{(n+1)m}$ or $F_{4m} \mid F_{(n-1)m}$. And $F_{4m} = F_{2m}L_{2m}$, then $L_{2m} \mid F_{4m} \mid \left(F^2_{nm}-F^2_m\right)$. By letting $m = 2^q$, we get $F^2_{2^q\cdot n} \equiv F^2_{2^q} \pmod{L_{2^{q+1}}}$. $\square$

Lemma 3.2. *For any positive integer q, $L_{2^{q+1}} \equiv 7 \pmod{10}$.*

Proof. We will proof this lemma by using induction. When $q = 1$, then $L_{2^{q+1}} = L_4 = 7 \pmod{10}$. Suppose that $L_{2^{q+1}} \equiv 7 \pmod{10}$ is true, then $L_{2^{q+2}} = L^2_{2^{q+1}} - 2 \equiv 7^2 - 2 \equiv 7 \pmod{10}$. Therefore, $L_{2^{q+1}} \equiv 7 \pmod{10}$ is true for any positive integer q. $\square$

Theorem 3.3. *The Diophantine triple $\{1,5,10\}$ cannot be extended to a $D(-1)$ quadruple $\{1,5,10,d\}$, for all integers $d > 10$.*

Proof. We only need to prove $10F^2_{2n_0}+9$ is not a perfect square for any positive integer n_0. Suppose there exists a positive integer l such that $l^2 = 10F^2_{2n_0}+9$.

If n_0 is odd, then $F^2_{2n_0} \equiv 1 \pmod 7$ by Lemma 3.1 for $q = 1$, then $l^2 = 10F^2_{2n_0}+9 \equiv 5 \pmod 7$. Thus, $1 = \left(\frac{l^2}{7}\right) = \left(\frac{5}{7}\right) = -1$ gave us a contradiction, therefore n_0 is even. Rewrite $2n_0$ in the form $2n_0 = 2^q\cdot n$ such that $q \geq 2$ and $2 \nmid n$. By Lemma 3.2, $L_{2^{q+1}} \equiv 7 \pmod{10}$, then

$\left(\frac{L_{2^{q+1}}}{5}\right) = \left(\frac{2}{5}\right) = -1$, then there exists an odd prime p such that $p \mid L_{2^{q+1}}$ and $\left(\frac{p}{5}\right) = -1$. Since $10F_{2^q}^2 + 9 = 2\left(5F_{2^q}^2 + 4\right) + 1 = 2L_{2^q}^2 + 1 = 2\left(L_{2^{q+1}} + 2\right) + 1 = 2L_{2^{q+1}} + 5$, then $1 = \left(\frac{l^2}{p}\right) = \left(\frac{10F_{2n_0}^2+9}{p}\right) = \left(\frac{10F_{2^q \cdot n}^2+9}{p}\right) = \left(\frac{10F_{2^q}^2+9}{p}\right) = \left(\frac{2L_{2^{q+1}}+5}{p}\right) = \left(\frac{5}{p}\right) = -1$, a contradiction.

In conclusion, then the Diophantine triple $\{1, 5, 10\}$ cannot be extended to a Diophantine quadruple $\{1, 5, 10, d\}$, for all integers $d > 10$. $\square$

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers. I*, Mathematika, A Journal of Pure and Applied Mathematics **13**, (1966) 204-216.

[2] E. Brown, *Sets in which $xy + k$ is always a square.*, Math. Comp. **45** (1985), 613–620.

[3] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arith. **65** (1993), 15–27.

[4] A. Dujella, *Complete solution of a family of simultaneous Pellian equations*, Acta Math. Inform. Univ. Ostraviensis **6** (1998), 59–67.

[5] A. Dujella, A. Filipin and C. Fuchs, *Effective solution of the $D(-1)$-quadruple conjecture*, Acta Math. Inform. Univ. Ostraviensis **128** (2007), no. 4, 319–338.

[6] A. Dujella and C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, Journal of the London Mathematical Society **71** (2005), no. 01, 33–52.

[7] A. Filipin, *Non-extendibility of $D(-1)$-triples of the form $\{1, 10, c\}$*, International journal of mathematics and mathematical sciences **2005** (2005), no. 14, 2217–2226.

[8] P. Gibbs, *A generalised stern-brocot tree from regular Diophantine quadruples*, Arxiv preprint math/9903035 (1999).

[9] H. Gupta and K. Singh, *On k-triad sequences*, International journal of mathematics and mathematical sciences **8** (1985), no. 4, 799–804.

[10] O. Kihel, *On the extendibility of the P_{-1}-set $\{1, 2, 5\}$*, Fibonacci Quart **38** (2000), no. 5, 464–466.

[11] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, John Wiley & Sons, Inc., 2001.

[12] S. P. Mohanty and A. M. S. Ramasamy, *The simultaneous Diophantine equations $5y^2 - 20 = x^2$ and $2y^2 + 1 = z^2$*, Journal of Number Theory **18** (1984), no. 3, 356–359.

[13] S. P. Mohanty and A. M. S. Ramasamy, *On $P_{r,k}$ sequences*, Fibonacci Quarterly **23** (1985), no. 1, 36–44.

[14] F. S. Abu. Muriefah and A. Al-Rashed, *On the extendibility of the Diophantine triple $\{1, 5, c\}$*, International Journal of Mathematics and Mathematical Sciences **2004** (2004), no. 33, 1737–1746.

[15] P. G. Walsh, *On two classes of simultaneous Pell equations with no solutions*, Mathematics of Computation **68** (1999), no. 225, 385–388.

MSC2010: 11B39, 11D09

E-mail address: zhang5y@cmich.edu

Department of Mathematics, Central Michigan University, Mount Pleasant, Michigan

E-mail address: gross1gw@cmich.edu

Department of Mathematics, Central Michigan University, Mount Pleasant, Michigan