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

Yifan Zhang

A thesis submitted in partial fulfillment of
the requirements for the degree of
Master of Arts in Mathematics

Department of Mathematics

Central Michigan University
Mount Pleasant, Michigan
October 2011

Accepted by the Faculty of the College of Graduate Studies,

Central Michigan University, in partial fulfillment of

the requirements for the master's degree

Thesis Committee:

George Grossman — Committee Chair

Sidney Graham — Faculty Member

Yeonhyang Kim — Faculty Member

Date: 03/02/12

Dean
College of Graduate Studies

Date: 5/10/12

Committee:

George Grossman, Ph.D.,Chair

Sidney Graham, Ph.D.

Yeonhyang Kim, Ph.D.

ACKNOWLEDGEMENTS

I would like to thank my parents for their support and encouragement. I would like to thank the members of the thesis committee: Chair Dr. Grossman, Dr. Graham and Dr. Kim for their kind assistance and helpful suggestions.

ABSTRACT

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

by Yifan Zhang

In this paper, we will point out the sufficient and necessary conditions, given integers a, b and c, when there exists integers n, α, β and γ such that $ab+n=\alpha^2$, $ac+n=\beta^2$ and $bc+n=\gamma^2$. The triple $\{a,b,c\}$ having this property is called a Diophantine triple with property $D(n)$. Similarly, this definition can be extended for the quadruple $\{a,b,c,d\}$. We will also discuss the existence of some special Diophantine triples and quadruples. Furthermore, we will prove the nonextendibility of Diophantine triples $\{1,2,5\}$ and $\{1,5,10\}$ by using elementary methods when $n=-1$.

TABLE OF CONTENTS

CHAPTER I

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 $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$ 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 $\{1,3,8,120,\frac{777480}{8288641}\}$ and then 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 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, Gupta & Singh and Mohanty & Ramasamy all in 1985. In 1993, Dujella 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 proved the nonextendibility of the Diophantine $D(-1)$ triple $\{1,2,5\}$. Walsh and Kihel also independently proved that in 1999 and 2000 respectively. In 1984, Mohanty & Ramasamy proved that the Diophantine $D(-1)$ triple $\{1,5,10\}$ can not be extended to a $D(-1)$ quadruple. Furthermore, Brown proved that $\left\{n^2+1,(n+1)^2+1,(2n+1)^2+4\right\}$ 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 was the first mathematician who proved the nonextendibility 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. In 2005, Filipin proved the nonextendibility of $\{1,10,c\}$.

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

CHAPTER II

MAIN THEOREM

Definition 2.1. *For three given positive integers a, b, c with $a < b < c$, $\{a,b,c\}$ is called a Diophantine triple with the property $D(n)$ if there exist positive integers α, β, γ and an integer n satisfying*

$$\begin{cases} \alpha^2 = ab+n, \\ \beta^2 = ac+n, \\ \gamma^2 = bc+n. \end{cases} \tag{2.1}$$

Example 2.2. *Given $\{a,b,c\}=\{12,28,42\}$, then $(\alpha,\beta,\gamma)=(1,13,29)$ with $n=-335$ and $(\alpha,\beta,\gamma)=(11,17,31)$ with $n=-215$ satisfying:*

$$\begin{cases} \alpha^2 = 1^2 = 12\times 28-335 = ab+n, \\ \beta^2 = 13^2 = 12\times 42-335 = ac+n, \\ \gamma^2 = 29^2 = 28\times 42-335 = bc+n. \end{cases} \quad \begin{cases} \alpha^2 = 11^2 = 12\times 28-215 = ab+n, \\ \beta^2 = 17^2 = 12\times 42-215 = ac+n, \\ \gamma^2 = 31^2 = 28\times 42-215 = bc+n. \end{cases}$$

Remark 2.3. *For three given positive integers α, β, γ with $\alpha < \beta < \gamma$, there can exist more than one Diophantine triple satisfying (2.1) with the property $D(n)$ (i.e. have different $n's$).*

Example 2.4. *Given $(\alpha,\beta,\gamma) = (3,11,31)$, then exist Diophantine triples $\{1,8,120\}$ with $n=1$, $\{8,28,42\}$ with $n=-215$ and $\{14,34,42\}$ with $n=-467$ satisfying (2.1).*

Theorem 2.5. *If $a+b+c$ is even with $a<b<c$, then $\{a,b,c\}$ is a Diophantine triple with the property $D(n)$ where*

$$\begin{cases} \alpha = \frac{1}{2}(a+b-c) \\ \beta = \frac{1}{2}(c+a-b) \\ \gamma = \frac{1}{2}(b+c-a) \end{cases} \quad \text{and } n = \frac{1}{4}\left(a^2+b^2+c^2-2ab-2ac-2bc\right).$$

Proof. Since $a+b+c$ is even, $a+b-c$, $c+a-b$ and $b+c-a$ are all even. Then α, β and γ are all integers.

Let $n=\frac{1}{4}\left(a^2+b^2+c^2-2ab-2ac-2bc\right)$,

then $ab+n=ab+\frac{1}{4}\left(a^2+b^2+c^2-2ab-2ac-2bc\right)=\left[\frac{1}{2}(a+b-c)\right]^2=\alpha^2$.

Similarly, we can get $ac+n=\beta^2$ and $bc+n=\gamma^2$. The results for β and γ follow easily.

Then the triple $\{a,b,c\}$ is a Diophantine triple with the property $D(n)$. □

Remark 2.6. *For any given three positive integers α,β,γ with $\alpha<\beta<\gamma$, there exist at lease two Diophantine triples $\{a,b,c\}$ that satisfy* (2.1). *The general solutions are given by*

$$\begin{cases} a=\alpha+\beta \\ b=\alpha+\gamma \\ c=\beta+\gamma \end{cases}, n=-(\alpha\beta+\alpha\gamma+\beta\gamma) \text{ and } \begin{cases} a=\beta-\alpha \\ b=\gamma-\alpha \\ c=\beta+\gamma. \end{cases} \quad n=\alpha\beta+\alpha\gamma-\beta\gamma$$

Proof. These can easily be proved by checking the equality of $ab+n$ and α^2, $ac+n$ and β^2, $bc+n$ and γ^2.

For example, $ab+n=(\alpha+\beta)(\alpha+\gamma)+n=\alpha^2+\alpha\gamma+\alpha\beta+\beta\gamma-(\alpha\gamma+\alpha\beta+\beta\gamma)=\alpha^2$. □

These general solutions could be explained by matrix equations as well:

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} = \begin{bmatrix} \alpha+\beta \\ \alpha+\gamma \\ \beta+\gamma \end{bmatrix}, \quad \text{or}$$

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} -1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} = \begin{bmatrix} \beta-\alpha \\ \gamma-\alpha \\ \beta+\gamma \end{bmatrix}, \quad \text{and}$$

$$\begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{bmatrix}\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \frac{1}{2}\begin{bmatrix} a+b-c \\ a-b+c \\ -a+b+c \end{bmatrix}.$$

The main result is

Theorem 2.7. *Let a, b, c be three positive integers with $a < b < c$, such that a, b, c are all odd or all even or only one of them is odd. Then exists an integer n such that $\{a,b,c\}$ is a Diophantine triple with the property $D(n)$ if and only if there exists positive integers λ, P_b, P_c such that $\lambda = \frac{b(c-a)}{4P_b} + P_b = \frac{c(b-a)}{4P_c} + P_c$. Moreover, $n = \lambda^2 - bc$.*

Proof. ($\Rightarrow$) Suppose that a, b, c are three positive integers with $a < b < c$, the number of even integers in $\{a,b,c\}$ is not one, and $\{a,b,c\}$ is a Diophantine triple. By assumption there exist integers α, β, γ and an integer n such that $\begin{cases} \alpha^2 = ab+n, \\ \beta^2 = ac+n, \\ \gamma^2 = bc+n. \end{cases}$

Now, denote $P_b = \frac{\gamma-\alpha}{2}$, $P_c = \frac{\gamma-\beta}{2}$. Subtracting the first equation from the third one, we get $b(c-a) = \gamma^2 - \alpha^2$.

The number of even integers in $\{a,b,c\}$ is not one,

$\Rightarrow 2 | b(c-a) = \gamma^2 - \alpha^2 = (\gamma+\alpha)(\gamma-\alpha)$

$\Rightarrow 2 | \gamma-\alpha$ or $2 | \gamma+\alpha$

$\Rightarrow 2 | \gamma-\alpha$ and $2 | \gamma+\alpha$

$\Rightarrow P_b = \frac{\gamma-\alpha}{2}$ is an integer and $\frac{b(c-a)}{4P_b} = \frac{\gamma^2-\alpha^2}{4\frac{\gamma-\alpha}{2}} = \frac{\gamma+\alpha}{2}$ is an integer

$\Rightarrow \lambda = \frac{b(c-a)}{4P_b} + P_b$ is an integer.

Similarly, P_c and $\frac{c(b-a)}{4P_c}$ are integers by same argument.

Since $\frac{b(c-a)}{4P_b} + P_b = \frac{\gamma^2-\alpha^2}{4\frac{\gamma-\alpha}{2}} + \frac{\gamma-\alpha}{2} = \frac{\gamma+\alpha}{2} + \frac{\gamma-\alpha}{2} = \gamma$ and $\frac{c(b-a)}{4P_c} + P_c = \frac{\gamma^2-\beta^2}{4\frac{\gamma-\beta}{2}} + \frac{\gamma-\beta}{2} = \frac{\gamma+\beta}{2} + \frac{\gamma-\beta}{2} = \gamma$, $\frac{b(c-a)}{4P_b} + P_b = \frac{c(b-a)}{4P_c} + P_c$.

($\Leftarrow$) Suppose that a, b, c are three positive integers with $a<b<c$, the number of even integers in $\{a,b,c\}$ is not one and there exist positive integers λ, P_b, P_c such that $\lambda=\frac{b(c-a)}{4P_b}+P_b=\frac{c(b-a)}{4P_c}+P_c$.

Let $\gamma=\lambda$, $\alpha=\left|\frac{b(c-a)}{4P_b}-P_b\right|$ and $\beta=\left|\frac{c(b-a)}{4P_c}-P_c\right|$, $n=\lambda^2-bc$, then

$ab+n=\lambda^2+ab-bc=\left(\frac{b(c-a)}{4P_b}+P_b\right)^2-b(c-a)=\left(\frac{b(c-a)}{4P_b}\right)^2+\frac{b(c-a)}{2}+{P_b}^2-b(c-a)=\left(\frac{b(c-a)}{4P_b}\right)^2-\frac{b(c-a)}{2}+{P_b}^2=\left(\frac{b(c-a)}{4P_b}-P_b\right)^2=\alpha^2$,

$ac+n=\lambda^2+ac-bc=\left(\frac{c(b-a)}{4P_c}+P_c\right)^2-c(b-a)=\left(\frac{c(b-a)}{4P_c}\right)^2+\frac{c(b-a)}{2}+{P_c}^2-c(b-a)=\left(\frac{c(b-a)}{4P_c}\right)^2-\frac{c(b-a)}{2}+{P_c}^2=\left(\frac{c(b-a)}{4P_c}-P_c\right)^2=\beta^2$,

and, by above, $bc+n=\lambda^2=\gamma^2$. □

Remark 2.8. *If a, b, c are three positive integers with $a<b<c$ and only one of them is even, then $\{a,b,c\}$ is a Diophantine triple if and only if there exist positive integers λ, P_b, P_c such that $\lambda=\frac{b(c-a)}{P_b}+P_b=\frac{c(b-a)}{P_c}+P_c$. Moreover, $n=\frac{\lambda^2}{4}-bc$.*

Proof. ($\Rightarrow$) Denote $P_b=\gamma-\alpha$ and $P_c=\gamma-\beta$.

It is clear that P_b and P_c are positive integers. Since $\frac{b(c-a)}{P_b}+P_b=\frac{\gamma^2-\alpha^2}{\gamma-\alpha}+\gamma-\alpha=\gamma+\alpha+\gamma-\alpha=2\gamma$ and $\frac{c(b-a)}{P_c}+P_c=\frac{\gamma^2-\beta^2}{\gamma-\beta}+\gamma-\beta=\gamma+\beta+\gamma-\beta=2\gamma$, $\frac{b(c-a)}{P_b}+P_b=\frac{c(b-a)}{P_c}+P_c$.

($\Leftarrow$) Since a, b, c are three positive integers with $a<b<c$ and only one of them is even, then at least one of $b(c-a)$ and $c(b-a)$ is odd. Without loss of generality, we assume that $c(b-a)$ is odd, then P_c and $\frac{c(b-a)}{P_c}$ are odd. Thus λ is even, then $\frac{b(c-a)}{P_b}$ and P_b are both odd or even.

Let $\gamma=\frac{\lambda}{2}$, $\alpha=\frac{1}{2}\left|\frac{b(c-a)}{P_b}-P_b\right|$, $\beta=\frac{1}{2}\left|\frac{c(b-a)}{P_c}-P_c\right|$ and $n=\frac{\lambda^2}{4}-bc$, therefore α, β and γ are all positive integers. Then we have

$ab+n=\frac{\lambda^2}{4}-bc+ab=\frac{1}{4}\left(\frac{b(c-a)}{P_b}+P_b\right)^2-b(c-a)=\frac{1}{4}\left(\frac{b(c-a)}{P_b}\right)^2+\frac{b(c-a)}{2}+\frac{{P_b}^2}{4}-b(c-a)=\frac{1}{4}\left(\frac{b(c-a)}{P_b}\right)^2-\frac{b(c-a)}{2}+\frac{{P_b}^2}{4}=\frac{1}{4}\left(\frac{b(c-a)}{P_b}-P_b\right)^2=\alpha^2$,

$$ac+n=\frac{\lambda^2}{4}-bc+ac=\frac{1}{4}\left(\frac{c(b-a)}{P_c}+P_c\right)^2-c(b-a)=\frac{1}{4}\left(\frac{c(b-a)}{P_c}\right)^2+\frac{c(b-a)}{2}+\frac{P_c^2}{4}-$$

$$c(b-a)=\frac{1}{4}\left(\frac{c(b-a)}{P_c}\right)^2-\frac{c(b-a)}{2}+\frac{P_c^2}{4}=\frac{1}{4}\left(\frac{c(b-a)}{P_c}-P_c\right)^2=\beta^2,$$

and, by above, $bc+n=\frac{\lambda^2}{4}=\gamma^2$. □

CHAPTER III

SEVERAL APPLICATIONS

Lemma 3.1. *If a, b, c are three odd positive integers with $a < b < c$ and $\{a,b,c\}$ is a Diophantine triple with the property $D(n)$, then $4|c-b$, $4|b-a$ and $4|c-a$.*

Proof. By Definition 2.1, there exist positive integers α, β, γ and integer n so that

$$\begin{cases} \alpha^2 = ab+n, \\ \beta^2 = ac+n, \\ \gamma^2 = bc+n. \end{cases}$$

Then $2|c-b \Rightarrow 2|a(c-b) = (ac+n)-(ab+n) = \beta^2-\alpha^2 = (\beta-\alpha)(\beta+\alpha)$

$\Rightarrow 2|\beta-\alpha$ or $2|\beta+\alpha$

$\Rightarrow 2|\beta-\alpha$ and $2|\beta+\alpha$

$\Rightarrow 4|(\beta-\alpha)(\beta+\alpha) = \beta^2-\alpha^2 = a(c-b)$

$\Rightarrow 4|c-b$.

Similarly, $4|b-a$ and $4|c-a$. □

Corollary 3.2. *If $c > 7$ is a prime number, then $\{3,7,c\}$ is never a Diophantine triple with the property $D(n)$ for any integer n.*

Proof. Suppose that $\{3,7,c\}$ is a Diophantine $D(n)$ triple, then by Theorem 2.7, there exists positive integers λ, P_b, P_c such that $\lambda = \frac{7(c-3)}{4P_b} + P_b = \frac{4c}{4P_c} + P_c = \frac{c}{P_c} + P_c$.

Then $\frac{c}{P_c} = \lambda - P_c$ is an integer, thus $P_c|c$.

Consider that c is a prime number, then $P_c = 1$ or $P_c = c$ and $\lambda = c+1$.

According to Lemma 3.1, suppose that $c = 3+4k$ with integer $k > 1$, then we have $\lambda = \frac{7k}{P_b} + P_b = c+1 = 3+4k+1 = 4(k+1)$.

Let $A=\frac{7k}{P_b}$, $B=P_b$, we have $A+B=4(k+1)$ and $AB=7k$. So

$(A-B)^2=(A+B)^2-4AB=[4(k+1)]^2-28k=16k^2+32k+16-28k=4\left(4k^2+k+4\right)$.

Thus $A-B$ is even and $\frac{A-B}{2}$ is an integer, we have $\left(\frac{A-B}{2}\right)^2=4k^2+k+4$.

Since $(2k+1)^2-\left(4k^2+k+4\right)=\left(4k^2+4k+1\right)-\left(4k^2+k+4\right)=3(k-1)>0$, we obtain that $(2k)^2=4k^2<\left(\frac{A-B}{2}\right)^2=4k^2+k+4<4k^2+4k+1=(2k+1)^2$, which contradicts the fact that $\frac{A-B}{2}$ is an integer.

Thus if $c>7$ is a prime number, then $\{3,7,c\}$ is never a Diophantine triple with the property $D(n)$ for any integer n. □

Remark 3.3. *If one of c and d is a prime number larger than 7, then for any integer n, the quadruple* $\{3,7,c,d\}$ *is never a Diophantine quadruple with the property* $D(n)$.

Proof. This could be proved by directly applying Corollary 3.2. □

Corollary 3.4. *If a, b, c are three odd positive integers with* $a<b<c$, $\frac{c-a}{4}$ *and* $\frac{b-a}{8}$ *are odd integers, then for any integer n, the triple* $\{a,b,c\}$ *will never be a Diophantine triple with the property* $D(n)$.

Proof. Suppose that exists integer n such that $\{a,b,c\}$ is a Diophantine triple with the property $D(n)$. Then by Theorem 2.7, there exist positive integers λ, P_b, P_c such that $\lambda=\frac{b(c-a)}{4P_b}+P_b=\frac{c(b-a)}{4P_c}+P_c$.

Since $\frac{b(c-a)}{4P_b}\cdot P_b=\frac{b(c-a)}{4}$ is odd, $\frac{b(c-a)}{4P_b}$ and P_b are both odd integers, then $\lambda=\frac{b(c-a)}{4P_b}+P_b$ is even.

On the other hand, $\frac{b-a}{8}$ is odd implies that $\frac{b-a}{4}$ is even and $4\nmid\frac{b-a}{4}$.

Then $2\mid\frac{c(b-a)}{4P_c}\cdot P_c$ and $4\nmid\frac{c(b-a)}{4P_c}\cdot P_c$.

Then $2|\frac{c(b-a)}{4P_c}$ and $2\nmid P_c$ or $2\nmid \frac{c(b-a)}{4P_c}$ and $2|P_c$, then $\lambda = \frac{c(b-a)}{4P_c} + P_c$ is odd, which contradicts λ is even. □

Remark 3.5. *If a, b, c are three odd positive integers with $a < b < c$, $\frac{c-a}{8}$ and $\frac{b-a}{4}$ are odd integers, then for any integer n, the triple $\{a,b,c\}$ will never be a Diophantine triple with the property $D(n)$.*

Proof. The proof will be the same as Corollary 3.4. □

Corollary 3.6. *If a is an odd positive integer, then for any positive integer k_1, k_2, triple $\{a, a+8+16k_1, a+4+8k_2\}$ is never a Diophantine triple with the property $D(n)$ for any integer n.*

Proof. Since $\frac{1}{4}(a+4+8k_2-a) = 1+2k_2$ and $\frac{1}{8}(a+8+16k_1-a) = 1+2k_1$ are both odd, by Corollary 3.4 and Remark 3.5, $\{a, a+8+16k_1, a+4+8k_2\}$ is never a Diophantine triple with the property $D(n)$. □

Corollary 3.7. *If there exist positive integer m, k satisfying $0 < m < \frac{k-1}{2}$ and $\frac{3k(k-1)}{2m}$ is even, and $a = \frac{3k(k-1)}{2m} - (2k+1) - 2m$, then $\{a, a+4, a+4k\}$ is a Diophantine triple with the property $D\Big((4k-1)^2 + 2a(2k-1)\Big)$.*

Proof. Suppose there exist positive integers m, k satisfying $0 < m < \frac{k-1}{2}$ and $\frac{3k(k-1)}{2m}$ is even. Let $P_b = k-2m$, $P_c = 1$, $a = \frac{3k(k-1)}{2m} - 2k - 1 - 2m = \frac{3k^2-3k-4mk-2m-4m^2}{2m}$, therefore P_b is a positive integer and a is an odd integer. Then

$$\begin{aligned}
&\frac{b(c-a)}{4P_b} + P_b \\
&= \frac{(a+4)\cdot 4k}{4P_b} + P_b \\
&= \frac{3k^2-3k-4mk-2m-4m^2+8m}{2m} \cdot \frac{k}{k-2m} + k - 2m
\end{aligned}$$

$$= \frac{\left(3k^2-3k-4mk-4m^2+6m\right)k}{2m(k-2m)} + k - 2m$$

$$= \frac{(k-2m)(3k+2m-3)k}{2m(k-2m)} + k - 2m$$

$$= \frac{(3k+2m-3)k}{2m} + k - 2m$$

$$= \frac{3k^2+2mk-3k+2mk-4m^2}{2m}$$

$$= \frac{3k^2+4mk-3k-4m^2}{2m}.$$

On the other hand,

$$\frac{c(b-a)}{4P_c} + P_c$$

$$= \frac{(a+4k)\cdot 4}{4P_c} + P_c$$

$$= a+4k+1$$

$$= \frac{3k^2-3k-4mk-2m-4m^2}{2m} + 4k + 1$$

$$= \frac{3k^2-3k-4mk-2m-4m^2+8mk+2m}{2m}$$

$$= \frac{3k^2-3k+4mk-4m^2}{2m}$$

Thus, $\frac{b(c-a)}{4P_b} + P_b = \frac{c(b-a)}{4P_c} + P_c$, and by Theorem 2.7,

$$n = \left(\frac{c(b-a)}{4P_c} + P_c\right)^2 - bc = (a+4k+1)^2 - (a+4)(a+4k) = (4k-1)^2 + 2a(2k-1)$$

such that $\{a, a+4, a+4k\}$ is a Diophantine triple with the property $D(n)$. □

Example 3.8. *Suppose that $k = 5$ in Corollary 3.7. If there exists an integer n such that $\{a, a+4, a+20\}$ is a Diophantine triple with the property $D(n)$, then the integer m should satisfy that $\frac{3\cdot 5\cdot 4}{2\cdot m}$ is even and $0 < m < 2$. Thus $m = 1$, $a = 17$, $\{17, 21, 37\}$ is a Diophantine triple with the property $D(667)$.*

Remark 3.9. *For any positive integer m, $\{4m+1, 4m+5, 12m^2+20m+5\}$ is a Diophantine triple with the property $D(n)$ where $n = 144m^4 + 432m^3 + 404m^2 + 120m + 11$.*

Proof. Let $P_b = m+1$, $P_c = 1$, then $\frac{c(b-a)}{4P_c} + P_c = \frac{\left(12m^2+20m+5\right)\cdot 4}{4\cdot 1} + 1 = 12m^2 + 20m + 6$,

$$\frac{b(c-a)}{4P_b} + P_b$$
$$= \frac{(4m+5)\left(12m^2+16m+4\right)}{4(m+1)} + (m+1)$$
$$= (4m+5)(3m+1) + (m+1)$$
$$= 12m^2 + 19m + 5 + m + 1$$
$$= 12m^2 + 20m + 6$$

and $n = \left(\frac{c(b-a)}{4P_c} + P_c\right)^2 - bc$

$$= 4\left(6m^2+10m+3\right)^2 - \left(12m^2+20m+5\right)(4m+5)$$
$$= 144m^4 + 432m^3 + 404m^2 + 120m + 11.$$

Therefore, $\{4m+1, 4m+5, 12m^2+20m+5\}$ is a Diophantine triple with the property $D(n)$ where $n = 144m^4 + 432m^3 + 404m^2 + 120m + 11$. This is an infinite family of Diophantine triples $\{a,b,c\}$ when a, b and c are all odd. □

Example 3.10. *Let $m = 3$, then $\{13, 17, 173\}$ is a Diophantine triple with the property $D(27335)$. Let $m = 4$, then $\{17, 21, 277\}$ is a Diophantine triple with the property $D(71467)$.*

Remark 3.11. *For any positive integer m, $\{4m+3, 4m+7, 4m^2+12m+7\}$ is a Diophantine triple with the property $D(n)$ where $n = \left(4m^2+10m+3\right)\left(4m^2+10m+5\right)$.*

Proof. Let $P_b = m+1$, $P_c = 1$,then $\frac{c(b-a)}{4P_c} + P_c = 4m^2 + 12m + 8$,

$$\frac{b(c-a)}{4P_b} + P_b$$
$$= \frac{(4m+7)\left(4m^2+8m+4\right)}{4(m+1)} + (m+1)$$
$$= (4m+7)(m+1) + (m+1)$$
$$= 4m^2 + 12m + 8$$

and $n = \left(\frac{c(b-a)}{4P_c} + P_c\right)^2 - bc$

$$= \left(4m^2+12m+8\right)^2 - (4m+7)\left(4m^2+12m+7\right)$$
$$= 16m^4 + 80m^3 + 132m^2 + 80m + 15$$

$= (4m^2+10m+3)(4m^2+10m+5)$.

Therefore, $\{4m+3, 4m+7, 4m^2+12m+7\}$ is a Diophantine triple with the property with the property $D(n)$ where $n = (4m^2+10m+3)(4m^2+10m+5)$. □

Example 3.12. *Let $m = 1$, then $\{7, 11, 23\}$ is a Diophantine triple with the property $D(323)$. Let $m = 4$, then $\{19, 23, 119\}$ is a Diophantine triple with the property $D(11663)$.*

Corollary 3.13. *If a is an positive integer, p_1 and p_2 are two prime numbers with $a+4 < p_1 < p_2$, then for any integer n, $\{a, a+4, p_1, p_2\}$ is never a Diophantine quadruple with the property $D(n)$.*

Proof. Suppose that p_1 and p_2 are two prime numbers with $a+4 < p_1 < p_2$, if $\{a, a+4, p_1, p_2\}$ is a Diophantine quadruple with the property $D(n)$, then $\{a, a+4, p_1\}$ and $\{a, a+4, p_1\}$ are both Diophantine triples with the property $D(n)$.

Since $\{a, a+4, p_1\}$ is a Diophantine triple with the property $D(n)$,
$\lambda = \frac{b(c-a)}{4P_b} + P_b = \frac{c(b-a)}{4P_c} + P_c \Rightarrow \lambda = \frac{(a+4)(p_1-a)}{4P_b} + P_b = \frac{p_1}{P_c} + P_c$.

p_1 is a prime number implies that $P_c = 1$ or $P_c = p_1$, then $\lambda = p_1 + 1$,
$n = \lambda^2 - bc = (p_1+1)^2 - p_1(a+4)$.

Similarly, from $\{a, a+4, p_2\}$ is a Diophantine triple with the property $D(n)$, we can get $n = (p_2+1)^2 - p_2(a+4)$.

Thus, $(p_1+1)^2 - p_1(a+4) = (p_2+1)^2 - p_2(a+4)$, then we have
$(p_1-p_2)(p_1+p_2-a-2) = 0$, since $p_1 < p_2$, we obtain that $p_1 + p_2 = a+2$, which contradicts to $a+4 < p_1 < p_2$.

Therefore, for any integer n, $\{a, a+4, p_1, p_2\}$ is never a Diophantine quadruple with the property $D(n)$. □

Theorem 3.14. *If positive odd integers a, A and B satisfy $a > AB$, $A|3a$, $B|a+4$ and $a \equiv AB \pmod 4$, then there exists an integer n such that the triple $\left\{a, a+4, a+\frac{(a+4-AB)(3a+AB)}{4AB}\right\}$ is a Diophantine triple with the property $D(n)$.*

Proof. First of all, we can obtain that $4|a+4-AB$, $B|a+4-AB$ and $A|3a+AB$, then $4B|a+4-AB$, then $4AB|(a+4-AB)(3a+AB)$, thus $a+\frac{(a+4-AB)(3a+AB)}{4AB}$ is an integer.

According to Theorem 2.7, let $P_b = \frac{a+4-AB}{4}$, $P_c = 1$, then P_b is an integer.

Therefore $\frac{b(c-a)}{4P_b} + P_b$

$$= \frac{(a+4)\cdot\frac{(a+4-AB)(3a+AB)}{4AB}}{4\cdot\frac{a+4-AB}{4}} + \frac{a+4-AB}{4}$$

$$= \frac{(a+4)(3a+AB)}{4AB} + \frac{a+4-AB}{4}$$

$$= \frac{3a^2+12a+aAB+4AB+aAB+4AB-(AB)^2}{4AB}$$

$$= \frac{3a^2+12a+2aAB+8AB-(AB)^2}{4AB}$$

$$= \frac{(a+4)(3a+2AB)-(AB)^2}{4AB}$$

and $\frac{c(b-a)}{4P_c} + P_c$

$$= \frac{\left[a+\frac{(a+4-AB)(3a+AB)}{4AB}\right]\cdot 4}{4\cdot 1} + 1$$

$$= a+\frac{(a+4-AB)(3a+AB)}{4AB} + 1$$

$$= \frac{4aAB+3a^2+12a-3aAB+aAB+4AB-(AB)^2+4AB}{4AB}$$

$$= \frac{(a+4)(3a+2AB)-(AB)^2}{4AB}.$$

thus $\frac{b(c-a)}{4P_b} + P_b = \frac{c(b-a)}{4P_c} + P_c = \lambda$.

Then $n = \lambda^2 - bc$ with $b = a+4$ and $c = a+\frac{(a+4-AB)(3a+AB)}{4AB}$, and $\left\{a, a+4, a+\frac{(a+4-AB)(3a+AB)}{4AB}\right\}$ is a Diophantine triple with the property $D(n)$. We also note that a, $a+4$ and $a+\frac{(a+4-AB)(3a+AB)}{4AB}$ are all odd. □

Example 3.15. *If $a = 35$, then any element (A,B) in the set $\{(3,1),(7,1),(15,1),(1,3),(5,3)\}$ satisfies that $a > AB$, $A|3a$, $B|a+4$ and $a \equiv AB \pmod 4$.*

Thus triples $\{35,39,359\}$, $\{35,39,163\}$ *and* $\{35,39,83\}$ *are Diophantine triples with the property* $D(115599)$, $D(20539)$ *and* $D(3819)$ *respectively.*

In Chapter IV and V, we give the second and third main results.

CHAPTER IV

NONEXTENDIBILITY OF $\{1,2,5\}$

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

Definition 4.1. *$f(n)$ 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 $L(n+2)=L(n+1)+L(n)$.

The following basic properties of the Fibonacci and Lucas sequences will be used in our investigations. Suppose n is an integer and d is a positive integer, then we have

$(a)\ f(n)=\frac{1}{\sqrt{5}}\cdot\left[\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right]$,

$(b)\ L(n)=\left(\frac{1+\sqrt{5}}{2}\right)^n+\left(\frac{1-\sqrt{5}}{2}\right)^n$,

$(c)\ f(2n-1)f(2n+1)=f^2(2n)+1$,

$(d)\ f(2n)f(2n+2)=f^2(2n+1)-1$,

$(e)\ f(2n)=L(n)f(n)$,

$(f)\ L(2n)=L^2(n)-2\cdot(-1)^n$,

$(g)\ f(n+2d)=f(n+d)L(d)-(-1)^d f(n)$,

$(h)\ L(n+2d)=L(n+d)L(d)-(-1)^d L(n)$.

We have the following six lemmas.

Lemma 4.2. *$5f^2(2n)+4=L^2(2n)$ and $5f^2(2n+1)-4=L^2(2n+1)$.*

Proof. By using the property (a) and (b) above,

$5f^2(2n)+4$

$$
\begin{aligned}
&= \left[\left(\tfrac{1+\sqrt{5}}{2}\right)^{2n} - \left(\tfrac{1-\sqrt{5}}{2}\right)^{2n}\right]^2 + 4 \\
&= \left(\tfrac{1+\sqrt{5}}{2}\right)^{4n} - 2\left(\tfrac{1+\sqrt{5}}{2}\right)^{2n}\left(\tfrac{1-\sqrt{5}}{2}\right)^{2n} + \left(\tfrac{1-\sqrt{5}}{2}\right)^{4n} + 4 \\
&= \left(\tfrac{1+\sqrt{5}}{2}\right)^{4n} - 2 + \left(\tfrac{1-\sqrt{5}}{2}\right)^{4n} + 4 \\
&= \left(\tfrac{1+\sqrt{5}}{2}\right)^{4n} + 2 + \left(\tfrac{1-\sqrt{5}}{2}\right)^{4n} \\
&= \left[\left(\tfrac{1+\sqrt{5}}{2}\right)^{2n} + \left(\tfrac{1-\sqrt{5}}{2}\right)^{2n}\right]^2 \\
&= L^2(2n)
\end{aligned}
$$

and $5f^2(2n+1) - 4$

$$
\begin{aligned}
&= \left[\left(\tfrac{1+\sqrt{5}}{2}\right)^{2n+1} - \left(\tfrac{1-\sqrt{5}}{2}\right)^{2n+1}\right]^2 - 4 \\
&= \left(\tfrac{1+\sqrt{5}}{2}\right)^{4n+2} - 2\left(\tfrac{1+\sqrt{5}}{2}\right)^{2n+1}\left(\tfrac{1-\sqrt{5}}{2}\right)^{2n+1} + \left(\tfrac{1-\sqrt{5}}{2}\right)^{4n+2} - 4 \\
&= \left(\tfrac{1+\sqrt{5}}{2}\right)^{4n+2} + 2 + \left(\tfrac{1-\sqrt{5}}{2}\right)^{4n+2} - 4 \\
&= \left(\tfrac{1+\sqrt{5}}{2}\right)^{4n+2} - 2 + \left(\tfrac{1-\sqrt{5}}{2}\right)^{4n+2} \\
&= \left[\left(\tfrac{1+\sqrt{5}}{2}\right)^{2n+1} + \left(\tfrac{1-\sqrt{5}}{2}\right)^{2n+1}\right]^2 \\
&= L^2(2n+1).
\end{aligned}
$$

□

Lemma 4.3. *For any positive integer n, if $A = f(2n)$, then there are unique positive integers p_1 and p_2 such that $p_1 p_2 = A^2 + 1$ and $p_2 - p_1 = A$. Furthermore, $p_1 = f(2n-1)$ and $p_2 = f(2n+1)$.*

Proof. Let $p_1 = f(2n-1)$ and $p_2 = f(2n+1)$, then $p_1 p_2 = f(2n-1) f(2n+1) = f^2(2n) + 1 = A^2 + 1$ by the property (c) and $p_2 - p_1 = f(2n+1) - f(2n-1) = f(2n) = A$.

If there exist p_3 and p_4 with $0 < p_3 < p_4$ such that $p_3 p_4 = A^2 + 1$ and $p_4 - p_3 = A$, then $p_4 - p_3 = p_2 - p_1$, so $(p_4 + p_3)^2 = (p_4 - p_3)^2 + 4p_3 p_4 = (p_2 - p_1)^2 + 4p_1 p_2 = (p_2 + p_1)^2$, which implies that $p_4 + p_3 = p_2 + p_1$.

By adding and subtracting this equation and $p_4 - p_3 = p_2 - p_1$, we obtain that $p_4 = p_2$ and $p_3 = p_1$. Therefore, p_1 and p_2 are unique. □

Lemma 4.4. *For any positive integer A, the following statements are equivalent,*

(1) $\{1,5,A^2+1\}$ *is a Diophantine triple with the property* $D(-1)$.

(2) *There is a positive integer B such that* $5A^2+4=B^2$.

(3) *There is a positive integer n such that* $A=f(2n)$.

Proof. (1) $\Rightarrow$ (2)

For a positive integer A, suppose that $\{1,5,A^2+1\}$ is a Diophantine triple with the property $D(-1)$, then there is a $B\in N^+$ such that $B^2=5(A^2+1)-1=5A^2+4$.

(2) $\Rightarrow$ (3)

Suppose that A is the smallest positive integer satisfy following two properties:

(i) There is a positive integer B such that $5A^2+4=B^2$, and

(ii) $A\neq f(2n)$ for any positive integer n.

It is clear that $A\neq 1$, since $f(2\cdot 1)=1$, then $A>1$.

$5A^2+4=B^2$ implies that A, B are both even or odd and $A<B$, then $\frac{3A-B}{2}$ and $\frac{3B-5A}{2}$ are integers. Moreover, since $9A^2-B^2=9A^2-(5A^2+4)=4A^2-4>0$ and $9B^2-25A^2=9\cdot(5A^2+4)-25A^2=20A^2+36>0$, we obtain that $\frac{3A-B}{2}$ and $\frac{3B-5A}{2}$ are positive integers.

Since $5\left(\frac{3A-B}{2}\right)^2+4-\left(\frac{3B-5A}{2}\right)^2$

$=\frac{45A^2-30AB+5B^2}{4}+4-\frac{25A^2-30AB+9B^2}{4}$

$=\frac{20A^2-4B^2}{4}+4$

$=5A^2-B^2+4$

$=0.$

It follows that $5\left(\frac{3A-B}{2}\right)^2+4=\left(\frac{3B-5A}{2}\right)^2$.

If there is $k\in N^+$ such that $\frac{3A-B}{2}=f(2k)$, then, according to Lemma 4.3, there is a unique positive pair $p_1=f(2k-1)$, $p_2=f(2k+1)$ such that $p_1p_2=\left(\frac{3A-B}{2}\right)^2+1$ and $p_2-p_1=\frac{3A-B}{2}$.

Since $(B-2A)\left(\frac{B-A}{2}\right)$

$= \frac{2A^2-3AB+B^2}{2}$

$= \frac{4A^2-6AB+2B^2}{4}$

$= \frac{4A^2-6AB+B^2+5A^2+4}{4}$

$= \frac{9A^2-6AB+B^2}{4}+1$

$= \left(\frac{3A-B}{2}\right)^2+1$

and $\left(\frac{B-A}{2}\right)-(B-2A)=\frac{3A-B}{2}$.

It follows that $p_1 = f(2k-1) = B-2A$ and $p_2 = f(2k+1) = \frac{B-A}{2}$.

Then $A = \frac{3A-B}{2}+\frac{B-A}{2} = f(2k)+f(2k+1) = f(2k+2) = f(2(k+1))$, which contradicts the fact that $A \neq f(2n), \forall n \in N^+$.

Therefore $\forall k \in N^+$, $\frac{3A-B}{2} \neq f(2k)$, then $\frac{3A-B}{2} > A$ since A is the smallest positive integer satisfying those two properties (i) and (ii).

Then $A > B$, which contradicts the fact that $A < B$. Thus no such A exists.

In conclusion, for any positive integer A, if there exists a positive integer B such that $B^2 = 5A^2+4$, then there exists a positive integer n such that $A = f(2n)$.

$(3) \Rightarrow (1)$

For a positive integer A, suppose there is a positive integer n such that $A = f(2n)$.

Since $5\left(A^2+1\right)-1 = 5A^2+4 = 5f^2(2n)+4 = L^2(2n)$ by Lemma 4.2, $1\cdot\left(A^2+1\right)-1 = A^2$ and $1\cdot 5-1 = 2^2$, $\left\{1,5,A^2+1\right\}$ is a Diophantine triple with the property $D(-1)$.

Summing up, these three statements are equivalent. □

Lemma 4.5. *For any nonnegative integer q,*

$$f^2(3^q)+2f^2(2\cdot 3^q)+1 = \tfrac{1}{5}\left[L(2\cdot 3^q)+1\right]\left[2L(2\cdot 3^q)-1\right].$$

Proof. This lemma can be derived by the following calculation:

$$
\begin{aligned}
&5\left[f^2(3^q)+2f^2(2\cdot 3^q)+1\right]-\left[L(2\cdot 3^q)+1\right]\left[2L(2\cdot 3^q)-1\right]\\
&=5f^2(3^q)+10f^2(2\cdot 3^q)+5-2L^2(2\cdot 3^q)-L(2\cdot 3^q)+1\\
&=\left[5f^2(3^q)-4\right]+2\left[5f^2(2\cdot 3^q)+4\right]+2-2L^2(2\cdot 3^q)-L(2\cdot 3^q)\\
&=L^2(3^q)+2L^2(2\cdot 3^q)+2-2L^2(2\cdot 3^q)-L(2\cdot 3^q)\ \text{(By Lemma 4.2)}\\
&=L^2(3^q)+2-L(2\cdot 3^q)\\
&=L(2\cdot 3^q)-L(2\cdot 3^q)\ \text{(By the property } (f))\\
&=0.
\end{aligned}
$$

□

Lemma 4.6. *If n is a positive integer not divisible by 3, then*

$$f^2(2\cdot 3^q\cdot n)\equiv f^2(2\cdot 3^q)\,(\bmod\,[L(2\cdot 3^q)+1]).$$

Proof. We will first prove that

$$
f(2\cdot 3^q\cdot n)\equiv\begin{cases} f(2\cdot 3^q) & (\bmod\,[L(2\cdot 3^q)+1]) \quad n\equiv 1\,(\bmod 3),\\ -f(2\cdot 3^q) & (\bmod\,[L(2\cdot 3^q)+1]) \quad n\equiv 2\,(\bmod 3),\\ 0 & (\bmod\,[L(2\cdot 3^q)+1]) \quad n\equiv 0\,(\bmod 3).\end{cases} \tag{4.1}
$$

by using mathematical induction.

When $n=1$ and $n=2$, it is obvious that $f(2\cdot 3^q\cdot 1)\equiv f(2\cdot 3^q)\,(\bmod\,[L(2\cdot 3^q)+1])$ and $f(2\cdot 3^q\cdot 2)=L(2\cdot 3^q)f(2\cdot 3^q)\equiv -f(2\cdot 3^q)\,(\bmod\,[L(2\cdot 3^q)+1])$ by the property (e).

Suppose that for any positive integer k which equal or less than n, one of the above is true depending on the remainder when k is divided 3.

If $n\equiv 1\,(\bmod 3)$, then we have

$$
\begin{aligned}
&f(2\cdot 3^q\cdot(n+1))\\
&=f(2\cdot 3^q\cdot n)L(2\cdot 3^q)-(-1)^{2\cdot 3^q}f(2\cdot 3^q\cdot(n-1))\ \text{(By the property } (g))\\
&\equiv f(2\cdot 3^q)L(2\cdot 3^q)+0\,(\bmod\,[L(2\cdot 3^q)+1])\\
&\equiv -f(2\cdot 3^q)\,(\bmod\,[L(2\cdot 3^q)+1]).
\end{aligned}
$$

If $n \equiv 2 \pmod 3$, then we have

$f(2 \cdot 3^q \cdot (n+1))$

$= f(2 \cdot 3^q \cdot n) L(2 \cdot 3^q) - (-1)^{2 \cdot 3^q} f(2 \cdot 3^q \cdot (n-1))$ (By the property (g))

$\equiv -f(2 \cdot 3^q) L(2 \cdot 3^q) - f(2 \cdot 3^q) \pmod{[L(2 \cdot 3^q)+1]}$

$= -f(2 \cdot 3^q)[L(2 \cdot 3^q)+1] \pmod{[L(2 \cdot 3^q)+1]}$

$\equiv 0 \pmod{[L(2 \cdot 3^q)+1]}$.

If $n \equiv 0 \pmod 3$, then we have

$f(2 \cdot 3^q \cdot (n+1))$

$= f(2 \cdot 3^q \cdot n) L(2 \cdot 3^q) - (-1)^{2 \cdot 3^q} f(2 \cdot 3^q \cdot (n-1))$ (By the property (g))

$\equiv -f(2 \cdot 3^q \cdot n) - f(2 \cdot 3^q \cdot (n-1)) \pmod{[L(2 \cdot 3^q)+1]}$

$\equiv 0 - [-f(2 \cdot 3^q)] \pmod{[L(2 \cdot 3^q)+1]}$

$\equiv f(2 \cdot 3^q) \pmod{[L(2 \cdot 3^q)+1]}$.

Therefore, (4.1) is true for any positive integer n.

Thus $f^2(2 \cdot 3^q \cdot n) \equiv f^2(2 \cdot 3^q) \pmod{[L(2 \cdot 3^q)+1]}$ if n is a positive integer not divisible by 3. □

Lemma 4.7. *If* $q \geq 1$, $L(2 \cdot 3^q) \equiv 2 \pmod 4$.

Proof. We will first show that $L(3n)$

$= L(2n) L(n) - (-1)^n L(n)$ (By the property (h))

$= \left[L^2(n) - 2 \cdot (-1)^n\right] L(n) - (-1)^n L(n)$ (By the property (f))

$= L^3(n) - 3 \cdot (-1)^n L(n)$.

Then we will prove this lemma by using mathematical induction.

If $q = 1$, then $L(2 \cdot 3^q) = L(6) = 18 \equiv 2 \pmod 4$.

Suppose that $L(2 \cdot 3^q) \equiv 2 \pmod 4$ is true, then

$$L\left(2\cdot 3^{q+1}\right) = L^3\left(2\cdot 3^q\right) - 3\cdot(-1)^{2\cdot 3^q} L\left(2\cdot 3^q\right) \equiv 2^3 - 3\cdot 2 = 2 \pmod 4.$$

Thus $L(2\cdot 3^q) \equiv 2 \pmod 4$ for any integer $q \geq 1$. □

Before proving the theorem, we first introduce the Legendre symbol, $\left(\frac{a}{p}\right)$.

Definition 4.8. *Suppose p is an odd prime number and $p \nmid a$. Then we define $\left(\frac{a}{p}\right) = 1$ if there exists an integer x such that $x^2 \equiv a \pmod p$, and $\left(\frac{a}{p}\right) = -1$ if for any positive integer x, $x^2 \not\equiv a \pmod p$.*

Here are some properties related to Legendre symbol.

(*A*) If $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(*B*) If $p \nmid a$, then $\left(\frac{a^2}{p}\right) = 1$.

(*C*) If $p \nmid a$ and $p \nmid b$, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(*D*) If $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$.

Theorem 4.9. *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. Suppose that there is a positive integer d with $d > 5$ such that $\{1,2,5,d\}$ is the Diophantine quadruple with the property $D(-1)$. Then $d = A^2 + 1$ necessarily and there are positive integers n and l such that $A = f(2n)$ by Lemma 4.4 and

$$l^2 = 2d - 1 = 2\left(A^2+1\right) - 1 = 2A^2 + 1 = 2f^2(2n) + 1.$$

Write $2n$ in the form $2n = 2\cdot 3^q \cdot n_0$ with $q \geq 0$ and $3 \nmid n_0$.

If $q = 0$, then

$$f^2(2n)$$
$$= f^2\left(2\cdot 3^0 \cdot n_0\right)$$
$$\equiv f^2\left(2\cdot 3^0\right) \left(\bmod \left[L\left(2\cdot 3^0\right) + 1\right]\right) \text{ (By Lemma 4.6)}$$

$= f^2(2) \pmod 4$

$= 1 \pmod 4$.

Thus, $l^2 = 2f^2(2n) + 1 \equiv 3 \pmod 4$, a contradiction to the fact that the square of any integer is congruent to 0 or 1 modulo 4.

If $q \geq 1$, then $L(2 \cdot 3^q) \equiv 2 \pmod 4$ by Lemma 4.7. Thus $L(2 \cdot 3^q) + 1 \equiv 3 \pmod 4$.

Therefore, there is a prime number p such that $p | L(2 \cdot 3^q) + 1$ and $p \equiv 3 \pmod 4$. To see why, suppose that all primes dividing $L(2 \cdot 3^q) + 1$ are congruent to 1 modulo 4. The prime-power decomposition of $L(2 \cdot 3^q) + 1$ is $L(2 \cdot 3^q) + 1 = {q_1}^{e_1} {q_2}^{e_2} \cdots {q_k}^{e_k}$ where $e_i \geq 1$, $i = 1, 2, \cdots, k$, each q_i is a prime, $q_i \neq q_j$ for $i \neq j$, and $q_i \equiv 1 \pmod 4$. Then $L(2 \cdot 3^q) + 1 = {q_1}^{e_1} {q_2}^{e_2} \cdots {q_k}^{e_k} \equiv 1^{e_1} \cdot 1^{e_2} \cdots 1^{e_k} = 1 \pmod 4$, which contradicts the fact that $L(2 \cdot 3^q) + 1 \equiv 3 \pmod 4$.

Then we have

$1 = \left(\frac{l^2}{p}\right)$ (By the property (B))

$= \left(\frac{2f^2(2n)+1}{p}\right)$

$= \left(\frac{2f^2(2 \cdot 3^q \cdot k)+1}{p}\right)$

$= \left(\frac{2f^2(2 \cdot 3^q)+1}{p}\right)$ (By Lemma 4.6)

$= \left(\frac{-f^2(3^q)}{p}\right)$ (By Lemma 4.5)

$= \left(\frac{-1}{p}\right)\left(\frac{f^2(3^q)}{p}\right)$ (By the property (C))

$= \left(\frac{-1}{p}\right)$ (By the property (B))

However, $\left(\frac{-1}{p}\right) = -1$ when $p \equiv 3 \pmod 4$ by the property (D), a contradiction to the fact that $\left(\frac{-1}{p}\right) = 1$.

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

CHAPTER V

NONEXTENDIBILITY OF $\{1,5,10\}$

In this chapter, in order to prove our theorem, the Quadratic Reciprocity Theorem is required: if p and q are odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$. For example, $\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\frac{(p-1)(5-1)}{4}} = 1$.

We will also use the property (E): If p is an odd prime, then $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Lemma 5.1. *If q and n are positive integers, then*

$$f(2^q n) \equiv \begin{cases} f(2^q) & \left(\bmod L\left(2^{q+1}\right)\right) \quad n \equiv 1,3 \pmod 8, \\ f(2^q)L(2^q) & \left(\bmod L\left(2^{q+1}\right)\right) \quad n \equiv 2 \pmod 8, \\ 0 & \left(\bmod L\left(2^{q+1}\right)\right) \quad n \equiv 0,4 \pmod 8, \\ -f(2^q) & \left(\bmod L\left(2^{q+1}\right)\right) \quad n \equiv 5,7 \pmod 8, \\ -f(2^q)L(2^q) & \left(\bmod L\left(2^{q+1}\right)\right) \quad n \equiv 6 \pmod 8. \end{cases} \tag{5.1}$$

Moreover, if n is odd, $f^2(2^q n) \equiv f^2(2^q) \left(\bmod L\left(2^{q+1}\right)\right)$.

Proof. We will prove this lemma by using mathematical induction.

When $n = 1$ and $n = 2$, it is obvious that $f(2^q \cdot 1) \equiv f(2^q) \left(\bmod L\left(2^{q+1}\right)\right)$ and $f(2^q \cdot 2) \equiv f(2^q)L(2^q) \left(\bmod L\left(2^{q+1}\right)\right)$ by the property (e).

Suppose that for any positive integer k which is equal to or less than n, one of the above is true depending on the remainder when k is divided by 8.

If $n \equiv 1 \pmod 8$, then we have

$f(2^q(n+1))$

$= f(2^q n)L(2^q) - (-1)^{2^q} f(2^q(n-1))$ (By the property (g))

$\equiv f(2^q)L(2^q) \left(\bmod L\left(2^{q+1}\right)\right)$.

If $n \equiv 2 \pmod 8$, then we have

$$
\begin{aligned}
& f(2^q(n+1)) \\
& = f(2^q n)L(2^q) - (-1)^{2^q} f(2^q(n-1)) \text{ (By the property } (g)) \\
& \equiv f(2^q)L(2^q)L(2^q) - f(2^q) \left(\bmod L\left(2^{q+1}\right)\right) \\
& = f(2^q)\left[L^2(2^q) - 1\right] \\
& = f(2^q)\left[L\left(2^{q+1}\right) + 2 - 1\right] \text{ (By the property } (f)) \\
& \equiv f(2^q) \left(\bmod L\left(2^{q+1}\right)\right).
\end{aligned}
$$

The remaining parts for $n \equiv 3,4,5,6,7,0 \pmod 8$ can be similarly proved.

Thus, we proved (5.1) for arbitrary positive integer n and q. Then, moreover, we can obtain that $f^2(2^q n) \equiv f^2(2^q) \left(\bmod L\left(2^{q+1}\right)\right)$ from (5.1), when n is odd. □

Lemma 5.2. *For any positive integer q, $L\left(2^{q+1}\right) \equiv 7 \pmod{10}$.*

Proof. We will proof this lemma by using mathematical induction.

When $q = 1$, then $L\left(2^{q+1}\right) \equiv L(4) = 7 \pmod{10}$.

Suppose that $L\left(2^{q+1}\right) \equiv 7 \pmod{10}$ is true, then by the property (f), $L\left(2^{q+2}\right) = L^2\left(2^{q+1}\right) - 2 \equiv 7^2 - 2 \equiv 7 \pmod{10}$.

Therefore, $L\left(2^{q+1}\right) \equiv 7 \pmod{10}$ is true for any positive integer q. □

Theorem 5.3. *The Diophantine triple $\{1,5,10\}$ cannot be extended to a $D(-1)$ quadruple $\{1,5,10,d\}$, for all integers $d > 10$.*

Proof. Suppose that there is a positive integer d with $d > 10$ such that $\{1,5,10,d\}$ is the Diophantine quadruple with the property $D(-1)$, then $d = A^2 + 1$ necessarily and there are positive integers n and l such that $A = f(2n)$ by Lemma 4.4 and $l^2 = 10d - 1 = 10\left(A^2 + 1\right) - 1 = 10A^2 + 9 = 10f^2(2n) + 9$.

First we will prove that n is even.

Suppose that n is odd, thus, $f^2(2n) \equiv f^2(2) = 1 \pmod 7$ by Lemma 5.1 for $q = 1$.

Then $l^2 = 10f^2(2n) + 9 \equiv 5 \pmod 7$.

Thus, $1 = \left(\frac{l^2}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$ gives us a contradiction, therefore n is even.

Rewrite $2n$ in the form $2n = 2^q n_0$ such that $2 \le q$ and $2 \nmid n_0$.

Then we have $f^2(2n) = f^2(2^q n_0) \equiv f^2(2^q) \left(\bmod L\left(2^{q+1}\right)\right)$ by Lemma 5.1.

Let $f\left(2^{q-1}\right) = m$, then $L^2\left(2^{q-1}\right) = 5f^2\left(2^{q-1}\right) + 4 = 5m^2 + 4$ by Lemma 4.2,

$L(2^q) = L^2\left(2^{q-1}\right) - 2 = 5m^2 + 4 - 2 = 5m^2 + 2$ by the property (f),

$f^2(2^q) = L^2\left(2^{q-1}\right) f^2\left(2^{q-1}\right) = 5m^4 + 4m^2$ by the property (e), and

$L\left(2^{q+1}\right) = L^2(2^q) - 2 = \left(5m^2 + 2\right)^2 - 2 = 25m^4 + 20m^2 + 2$ by the property (f).

Then $l^2 = 10f^2(2n) + 9$

$= 10f^2(2^q n_0) + 9$

$\equiv 10f^2(2^q) + 9$ (By Lemma 5.1)

$= 10\left(5m^4 + 4m^2\right) + 9$

$= 2\left(25m^4 + 20m^2 + 2\right) + 5$

$= 2L\left(2^{q+1}\right) + 5$

$\equiv 5 \left(\bmod L\left(2^{q+1}\right)\right)$.

Since $\forall q \ge 2$, $L\left(2^{q+1}\right) \equiv 7 \pmod{10}$ by Lemma 5.2, then $\left(\frac{L\left(2^{q+1}\right)}{5}\right) = \left(\frac{2}{5}\right) = -1$, then there exists an odd prime number p such that $p \mid L\left(2^{q+1}\right)$ and $\left(\frac{p}{5}\right) = -1$. Otherwise, if the prime-power decomposition of $L\left(2^{q+1}\right)$ is $L\left(2^{q+1}\right) = {q_1}^{e_1} {q_2}^{e_2} \cdots {q_k}^{e_k}$ where $e_i \ge 1$, $i = 1, 2, \cdots, k$, each q_i is a prime, $q_i \ne q_j$ for $i \ne j$, and $\left(\frac{q_i}{5}\right) = 1$, then $\left(\frac{L\left(2^{q+1}\right)}{5}\right) = \left(\frac{{q_1}^{e_1}}{5}\right)\left(\frac{{q_2}^{e_2}}{5}\right) \cdots \left(\frac{{q_k}^{e_k}}{5}\right) = \left(\frac{q_1}{5}\right)^{e_1}\left(\frac{q_2}{5}\right)^{e_2} \cdots \left(\frac{q_k}{5}\right)^{e_k} = 1^{e_1} \cdot 1^{e_2} \cdots 1^{e_k} = 1$, which contradicts the fact that $\left(\frac{L\left(2^{q+1}\right)}{5}\right) = -1$.

Therefore $1 = \left(\frac{l^2}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$ gives us a contradiction.

Then the Diophantine triple $\{1,5,10\}$ cannot be extended to a Diophantine quadruple $\{1,5,10,d\}$, for all integers $d > 10$. □

REFERENCES

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

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

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

Dujella, A., Filipin, A., & Fuchs, C. (2007). Effective solution of the $D(-1)$-quadruple conjecture. *Acta Arith.*, *128*, 319–338.

Dujella, A., & Fuchs, C. (2005). Complete solution of a problem of Diophantus and Euler. *Journal of the London Mathematical Society*, *71*, 33–52.

Filipin, A. (2005). Non-extendibility of $D(-1)$-triples of the form$\{1, 10, c\}$. *International journal of mathematics and mathematical sciences*, *2005*, 2217–2226.

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

Gupta, H., & Singh, K. (1985). On k-triad sequences. *International journal of mathematics and mathematical sciences*, *8*, 799–804.

Kihel, O. (2000). On the extendibility of the P_{-1}-set $\{1, 2, 5\}$. *Fibonacci Quart*, *38*, 464–466.

Mohanty, S., & Ramasamy, A. (1984). The simultaneous Diophantine equations $5y^2-20=x^2$ and $2y^2+1=z^2$. *Journal of Number Theory*, *18*, 356–359.

Mohanty, S., & Ramasamy, A. (1985). On $P_{r,k}$ sequences. *Fibonacci Quarterly*, *23*, 36–44.

Muriefah, F., & Al-Rashed, A. (2004). On the extendibility of the Diophantine triple$\{1, 5, c\}$. *International Journal of Mathematics and Mathematical Sciences*, *2004*, 1737–1746.

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