Global Scientific JOURNALS

GSJ: Volume 10, Issue 5, May 2022, Online: ISSN 2320-9186

www.globalscientificjournal.com

ON DIOPHANTINE QUINTUPLE CONJECTURE

[1]Fahad Suleiman, [2]Abdullahi Mohammed Rashad & [3]Murtala Ahmed Maitama

[1,2,3]Department of Mathematics & Statistics

[1,2,3]Federal Polytechnic Kaura Namoda, Nigeria.

Corresponding email: fssalai@gmail.com

ABSTRACT

Diophantine problems gave fewer equations than unknowns and involve finding integers that solve simultaneously all equations. The simplest linear Diophantine equation takes the form $ax + by + c = 0$ *where* a, b, c *are given integers. In this paper, we presented some theorems that described solution to such equation. It also generalized various axioms of Diophantine m – tuples equation.*

Keywords: Diophantine equation, Integer, Solution, Theorem.

1.0 INTRODUCTION

The Greek mathematician Diophantus of Alexandria first studied the problem of finding four numbers such that the product of any two of them increased by unity is a perfect square. He found a set of four positive rationals with the this property: $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$. However, the first set of four positive integers with the above property. {1, 3, 8, 120}, was found by Fermat. Indeed, we have

$1 \cdot 3 + 1 = 2^2$, $1 \cdot 120 + 1 = 11^2$,
$1 \cdot 8 + 1 = 3^2$, $3 \cdot 120 + 1 = 19^2$,
$3 \cdot 8 + 1 = 5^2$, $8 \cdot 120 + 1 = 31^2$.

Euler found the infinite family such sets:

$\{a, b, a + b + 2r, 4r(r + a)(r + b)\}$, where $ab + 1 = r^2$. He was also able to add the fifth positive rational, 777480 / 8288641, to the Fermat set. In 2019, Stoll [1] proved that extension of Fermat's set to rational quintuples with the same property is unique.

In 1999, the first example of a set of six positive rationals with the property of Diophantus and Fermat was found by Gibbs [3, 2]:

{11/192, 35/192, 155/27, 512/27, 1235/48, 180873/16}.

These examples motivate the following definitions:

Definition 1.1: A set of m positive integers $\{a_1, a_2, \ldots, a_m\}$ is called a Diophantine m-tuple if $a_i \cdot a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$.

Definition 1.2: A set of m non-zero rationals $\{a_1, a_2, \ldots, a_m\}$ is called a rational Diophantine m-tuple if $a_i \cdot a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$.

It is natural to ask how large these sets, i.e. (rational) Diophantine tuples, can be. On the other hand, it seems that in the rational case we do not have even a widely accepted conjecture. In particular, no absolute upper bound for the size of rational Diophantine m-tuples is known.

In the integer case we have the following folklore "Diophantine quintuple conjecture".

Conjecture 1.1: There does not exist a Diophantine quintuple.

The first important result concerning this conjecture was proved in 1969 by Baker and Davenport [8]. Using Baker's theory on linear forms in logarithms of algebraic numbers and a reduction method based on continued fractions, they proved that if d is a positive integer such that $\{1, 3, 8, d\}$ forms a Diophantine quadruple, then $d = 120$. It implies that the Fermat's set $\{1, 3, 8, 120\}$ cannot be extended to a Diophantine quintuple. This problem was stated in 1967 by Gardner [4] and in 1968 by van Lint [5]. The same result was proved later, with different methods, by Kanagasabapathy & Ponnudurai [6].

2.0 BACKGROUND OF THE STUDY

In 1979 Arkin, Hoggatt and Strauss [7] proved that every Diophantine triple can be extended to a Diophantine quadruple. More precisely, let $\{a, b, c\}$ be a Diophantine triple and $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$, where r, s, t are positive integer. Define $d_+ = a + b + c + 2abc + 2rst$.

Then $\{a, b, c, d_+\}$ is a Diophantine quadruple. Indeed

$ad_+ + 1 = (at + rs)^2$, $bd_+ + 1 = (bs + rt)^2$, $cd_+ + 1 = (cr + st)^2$.

Now we can give a stronger version of the Diophantine quintuple conjecture

Conjecture 2.1: If $\{a, b, c, d\}$ is a Diophantine quadruple and $d > \max\{a, b, c\}$, then $d = d_+$.

It is clear that Conjecture 2.1 implies that there does not exist a Diophantine quintuple.

Baker & Davenport [8] verified Conjecture 2.1 for the Diophantine triple $\{1, 3, 8\}$. They verified the conjecture for the triple $\{2, 4, 12\}$ and Kedlaya [9] for the triples $\{1, 3, 120\}$, $\{1, 8, 120\}$, $\{1, 8, 15\}$, $\{1, 15, 35\}$, $\{1, 24, 35\}$ and $\{2, 12, 24\}$. In [10], the conjecture was verified for all triples of the form $\{k - 1, k + 1, 4k\}$ and $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$, respectively. Furthemore, in [11], Dujella & Pethő proved that the pair $\{1, 3\}$ cannot be extended to a Diophantine quintuple. In 2008, Fujita [12] proved that for $k \geq 2$, the Diophantine pair $\{k - 1, k + 1\}$ cannot be extended to a Diophantine quintuple.

Baker & Davenport [8] verified Conjecture 2.1 for the Diophantine triple $\{1, 3, 8\}$. They verified the conjecture for the triple $\{2, 4, 12\}$ and Kedlaya [9] for the triples $\{1, 3, 120\}$, $\{1, 8, 120\}$, $\{1, 8, 15\}$, $\{1, 15, 35\}$, $\{1, 24, 35\}$ and $\{2, 12, 24\}$. In [10], the conjecture was verified for all triples of the form $\{k - 1, k + 1, 4k\}$ and $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$, respectively. Furthemore, in [11], Dujella & Pethő proved that the pair $\{1, 3\}$ cannot be extended to a Diophantine quintuple. In 2008, Fujita [12] proved that for $k \geq 2$, the Diophantine pair $\{k - 1, k + 1\}$ cannot be extended to a Diophantine quintuple.

A Diophantine quadruple $D = \{a, b, c, d\}$, where $a < b < c < d$, is called regular if $d = d_+$. Equivalently, D is regular iff $(a + b - c - d)^2 = 4(ab + 1)(cd + 1)$

This equation is a quadratic equation in d. one root of this equation is d_+ and the other root is

$$d_- = a + b + c + 2abc - 2rst.$$

It is easy to check all "small" Diophantine quadruples are regular. Examples there are exactly 207 quadruples with $\max\{a, b, c, d\} < 10^6$ and all of them are regular.

Since the number of integer points on an elliptic curve $y^2 = (ax + 1)(bx + 1)(cx + 1)$ is finite, it follows that there does not exist an infinite set of positive integers with the property of Diophantus and Fermat. However, bounds for the size and for the number of solutions depend on a, b, c and, accordingly, they do not immediately yield an absolute bound for the size of such set.

Baker & Davenport [8] verified Conjecture 2.1 for the Diophantine triple $\{1, 3, 8\}$. They verified the conjecture for the triple $\{2, 4, 12\}$ and Kedlaya [9] for the triples $\{1, 3, 120\}$, $\{1, 8, 120\}$, $\{1, 8, 15\}$, $\{1, 15, 35\}$, $\{1, 24, 35\}$ and $\{2, 12, 24\}$. In [10], the conjecture was verified for all triples of the form $\{k - 1, k + 1, 4k\}$ and $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$, respectively. Furthemore, in [11], Dujella & Pethő proved that the pair $\{1, 3\}$ cannot be extended to a Diophantine quintuple. In 2008, Fujita [12] proved that for $k \geq 2$, the Diophantine pair $\{k - 1, k + 1\}$ cannot be extended to a Diophantine quintuple.

A Diophantine quadruple $D = \{a, b, c, d\}$, where $a < b < c < d$, is called regular if $d = d_+$. Equivalently, D is regular iff $(a + b - c - d)^2 = 4(ab + 1)(cd + 1)$

This equation is a quadratic equation in d. one root of this equation is d_+ and the other root is

$$d_- = a + b + c + 2abc - 2rst.$$

It is easy to check all "small" Diophantine quadruples are regular. Examples there are exactly 207 quadruples with max $\{a, b, c, d\} < 10^6$ and all of them are regular.

Since the number of integer points on an elliptic curve $y^2 = (ax + 1)(bx + 1)(cx + 1)$ is finite, it follows that there does not exist an infinite set of positive integers with the property of Diophantus and Fermat. However, bounds for the size and for the number of solutions depend on a, b, c and, accordingly, they do not immediately yield an absolute bound for the size of such set.

The first absolute bound ($m \leq 8$) for the size of Diophantine m-tuples was given in 2001 by Dujella [13]. In 2004, this result was significantly improved in [14]. The main results of [14] are the following theorems.

Theorem 2.1: There does not exist a Diophantine sextuple.

Theorem 2.2: There are only finitely many Diophantine quintuples.

Moreover, the result from Theorem 2.2 is effective. Namely, it was proved in [14] that all Diophantine quintuples Q satisfy $\max Q < 10^{10}$. This implies that there are at most 10^{1930} Diophantine quintuples. This bound was significantly improved by Fujita in [168] by showing that there exist at most 10^{276} Diophantine quintuples.

Theorems 2.1 and 2.2 improve results from [16] where it is proved that there does not exist a Diophantine 9-tuple and that there are only finitely many Diophantine 8-tuples.

Theorems 2.1 and 2.2 improve results from [16] where it is proved that there does not exist a Diophantine 9-tuple and that there are only finitely many Diophantine 8-tuples.

As in [16], the main idea was to prove Conjecture 2.1 for a wide class of Diophantine triples, namely, for triples satisfying some gap conditions. However, in [14] these gap conditions are much weaker than in [16]. Thus, the class of Diophantine triples for which Conjecture 2.1 can be proved is now so wide that in an arbitrary Diophantine quadruple (with sufficiently large elements), we may find a sub-triple belonging to that class. And this is just what is needed in order to prove Theorem 2.2.

In the proof of Conjecture 2.1 for a triple {a, b, c}, the problem is first transformed into solving systems of simultaneous Pellian equations. This reduces to finding intersection of binary recursive sequences. Next step is the determination of initial terms of these sequences, under assumption that they have nonempty intersection which induces a

solution of the original problem. This part is considerable improvement of the corresponding part of [16]. This improvement is due to new "gap principles".

Applying some congruence relations modulo c^2, lower bounds for solutions are obtained. In obtaining these bounds, it is necessary to assume that our triple satisfies some gap conditions, e.g. $b > 4a$ and $c > b^{2.5}$. Let us note that these conditions are much weaker then conditions used in [16], and this is due to more precise determination of the initial terms.

The comparison of these lower bounds with upper bounds obtained from the Baker's theory on linear forms in logarithms of algebraic numbers (the theorem of Baker and Wüstholz, or more recent theorem of Matveev) yields Theorem 2.2, and the comparison with upper bounds obtained from a theorem of Bennett on simultaneous approximations of algebraic numbers yields Theorem 2.1.

We also mention a result by Fujita [12], who proved that any Diophantine quintuple contains a regular Diophantine quadruple, i.e. if $\{a, b, c, d, e\}$ is a Diophantine quintuple and $a < b < c < d < e$, then $d = d_+$.

From the results of [12] and [13], it follows that any quintuple $\{a, b, c, d, e\}$ with $a < b < c < d < e$ must be of one of the following types:

i. $4a < b$ and $4ab + a + b < c < b^{3/2}$,

ii. $4a < b$ and $c = a + b + 2\sqrt{ab+1}$,

iii. $4a < b$ and $c > b^{3/2}$,

iv. $b < 4a$ and $c = a + b + 2\sqrt{ab+1}$.

Theorem 2.3: There does not exist a Diophantine quintuple.

The three new key arguments that lead to the proof are:

the definition of an operator on Diophantine triples and their classification;

the use of sharp lower bounds for linear forms in three logarithms obtained by applying a result due to Mignotte;

the use of new congruences in the case of Euler quadruples $\{a, b, a + b + 2r, 4r(r + a)(r + b)\}$.

Conjecture 2.1 still remains open. In that direction, [9] proved that any fixed Diophantine triple can be extended to a Diophantine quadruple in at most 11 ways by joining a fourth element exceeding the maximal element in the triple, while [14] improved that result by replacing 11 with 8.

3.0 VARIOUS GENERALIZATIONS

Theorem 3.1: Let $k \geq 3$ be an integer and let

$C(k) = \sup \{|S| : S \text{ is a k-th power Diophantine tuple}\}$.

Then $C(3) \leq 7$, $C(4) \leq 5$, $C(k) \leq 4$ for $5 \leq k \leq 176$, and $C(k) \leq 3$ for $k \geq 177$.

A slightly more general problem has been considered by [10]. Let N and $k \geq 3$ be positive integers. Let A and B be subsets of $\{1, 2, \ldots, N\}$ such that $ab + 1$ is a perfect k-th power whenever $a \in A$ and $b \in B$. What can be said about the cardinalities of the sets A and B? Gyarmati proved that $\min \{|A|, |B|\} \leq 1+(\log \log N)/\log(k-1)$.

In [12] estimates for the size of a set $D \subseteq \{1, 2, \ldots, N\}$ with the property that $ab + 1$ is a perfect power for all $a, b \in D$, $a \neq b$, are given. The best known bound is due to Fujita [12]: $|D| \ll (\log N)^{2/3} (\log \log N)^{1/3}$. Luca [18] showed that the abc-conjecture implies that $|D|$ is bounded by an absolute constant.

In [19], A. Kihel & O. Kihel consired a different generalization of the problem of Diophantus and Fermat to higher powers. A $P_n^{(k)}$-set of size m is a set $\{a_1, a_2, \ldots, a_m\}$ of distinct positive integers such that $\prod_{j \in J} a_j + n$ is a k-th power of an integer, for each $J \subseteq \{1, 2, \ldots, m\}$ where $|J| = k$. They proved that any $P_n^{(k)}$-set is finite.

3.1. POLYNOMIALS

Let n be a polynomial with integer coefficients. Let $D = \{a_1, a_2, \ldots, a_m\}$ be a set of m nonzero polynomials with integer coefficients satisfying the conditions that there does not exist a polynomial $p \in Z[X]$ such that $a_1/p, a_2/p, \ldots a_m/p$ and n/p are integers. The set D is called a polynomial D(n)-m-tuples if the product of any two of its distinct elements increased by n is a square of a polynomial with integer coefficients.

A natural question is how large such sets can be. Let us define $P_n = \sup \{|S| : S \text{ is a polynomial D(n)-tuple}\}$.

Theorem 2.2 implies that $P_1 = 4$. Moreover, all polynomial D(1) – quadruples are regular, i.e. Conjucture 2.1 is valid for polynomials with integer coefficients. [12] Proved that the same result is valid for polynomials with real coefficients. On the other hand, [11] showed that there are regular D (1) – quadruples in polynomials with complex coefficients. Indeed, the D(1) – quadruples

$\{\sqrt{(-3)}/2, -2\sqrt{(-3)}/3\ (x^2 - 1), (-3 + \sqrt{(-3)})/3\ x^2 + 2\sqrt{(-3)}/3, (3 + \sqrt{(-3)})/3\ x^2 + 2\sqrt{(-3)}/3\}$ is regular.

In [15] it follows that $P_n \leq 22$ for all polynomials n of degree 0. These results also give a bound for P_n in terms of the degree and the maximum of the coefficients of n.

Let us mention that a variant of the problem of Diophantus and Fermat for polynomials was first considered by [14]. He treated the classical case n = 1. Various polynomial Diophantine quadruples were systematically derived by Dujella [2, 3] and [17]. Here are some examples:

$\{4x, 25x + 1, 49x + 3, 144x + 8\}$ for $n = 16x + 1$;
$\{4, 9x^2 - 5x, 9x^2 + 7x + 2, 36x^2 + 4x\}$ for $n = 8x + 1$;
$\{2x + 3, 3x^2 + 4x + 2, 9x^2 + 10x + 3, 24x^2 + 26x + 7\}$ for $n = 9x^4 + 6x^3 - 19x^2 - 20x - 5$.

In [19], the author considered the higher power variant of the problem of Diophantus and Fermat for polynomials. Let K be an algebraically closed field of characteristic zero. They proved that for every $k \geq 3$ there exist a constant P(k), depending only on k, such that if $\{a_1, a_2, \ldots, a_m\}$ is a set of polynomials, not all of them constant, with coefficients in K, with the property that $a_i a_j + 1$ is a k-th power of an element of K[X] for $1 \leq i < j \leq m$, then $m \leq P(k)$. More precisely, they proved that:

$m \leq 5$ if $k = 3$;
$m \leq 4$ if $k = 4$;
$m \leq 3$ for $k \geq 5$;
$m \leq 2$ for k even and $k \geq 8$.

Furthermore, in [20], Dujella and Jurasic proved that $m \leq 10$ if $k = 2$. They also obtained an absolute upper bound for the size of a set of polynomials with the property that the product of any two elements plus 1 is a perfect power.

3.2 GAUSSIAN INTEGERS AND INTEGERS IN QUADRATIC FIELDS

Let $z = a + bi$ be a Gaussian integer. A set of m Gaussian integers is called a complex Diophantine m-tuple with the property D(z) if the product of any two of its distinct elements increased by z is a square of Gaussian integer. In [63], the problem of existence of complex Diophantine quadruples was considered.

It was proved that if b is odd or $a \equiv b \equiv 2 \pmod 4$, then there does not exist a complex Diophantine quadruple with the property D(a + bi). It is interesting that this condition is equivalent to the condition that a + bi is not representable as a difference of the squares of two Gaussian integers. In that way, this result becomes an analogue of Theorem 3.1, since an integer n is of the form 4k + 2 if and only if n is not representable as a difference of the squares of two integers.

It was also proved that if a + bi is not of the above form and $a + bi \notin \{2, -2, 1 + 2i, -1 - 2i, 4i, -4i\}$, then there exists at least one complex Diophantine quadruple with the property D(a + bi).

In [17], the researchers considered the analogous problem in the ring $Z[\sqrt{-2}]$. They proved that there exists a Diophantine quadruple with the property $D(a + b\sqrt{-2})$ if a and b satisfy some congruence conditions. Their result was improved in [16] and [14]. In [1], Gardener solved completely the analogous problem in the ring $Z[\sqrt{2}]$. She proved that there exist infinitely many Diophantine quadruples with the property $D(z)$ if and only if z can be represented as a difference of two squares in $Z[\sqrt{2}]$.

4.0 CONNECTIONS WITH FIBONACCI NUMBERS

4.1 Hoggatt-Bergum conjecture

There are many formulae for Diophantine quadruples with elements represented in terms of Fibonacci numbers. The most popular such quadruple was founded in 1977 by Hoggatt & Bergum [21]:

$\{F_{2k}, F_{2k+2}, F_{2k+4}, 4F_{2k+1} F_{2k+2}F_{2k+3}\}$.

Hoggatt & Bergum conjecture that the fourth element in the above set is unique. The conjecture was proved by [7] and this result also implies that if

$\{F_{2k}, F_{2k+2}, F_{2k+4}, d\}$ is a Diophantine quadruples, then d cannot be a Fibonacci number

The main step in the proof of Hoggatt-Bergum conjecture is a comparison of the upper bounds for solutions obtained from a theorem of Baker and Wüstholz with the lower bounds obtained from the congruence conditions modulo $2F_{2k} F_{2k+2}$. This comparison finishes the proof for $zxk > 48$. The statement for $2 \leq k \leq 48$ was proved by a version of the reduction procedure due to Baker & Davenport [8].

Motivated by the Hoggatt-Bergum set, several authors considered the question how large Diophantine tuples consisting of Fibonacci numbers can be. [4] Proved that if $\{F_{2n}, F_{2n+2}, F_k\}$ is a Diophantine triple, then $k = 2n + 4$ or $k = 2n - 2$ (when $n > 1$), except when $n = 2$, in which case $k = 1$ is also possible. Van Lint in [5] proved that there are only finitely many Diophantine quadruples consisting of Fibonacci numbers, and in [3] they proved that there are no such quadruples.

REFERNCES

1. M. Stoll, Diagonal genus 5 curves, elliptic curves over $Q(t)$, and rational diophantine quintuples, Acta Arith. 190 (2019), 239-261.

2. P. Gibbs, A generalised Stern-Brocot tree from regular Diophantine quadruples, XXX Mathematics Archive math.NT/9903035.

3. P. Gibbs, Some rational Diophantine sextuples, Glas. Mat. Ser. III 41 (2006), 195-203.

4. M. Gardner, Mathematical games, Scientific American 216 (1967), March 1967, p. 124; April 1967, p.119.

5. J. H. van Lint, On a set of diophantine equations, T. H.-Report 68 - WSK-03, Department of Mathematics, Technological University Eindhoven, Eindhoven, 1968.

6. P. Kanagasabapathy and T. Ponnudurai, The simultaneous Diophantine equations $y^2 - 3x^2 = -2$ and $z^2 - 8x^2 = -7$, Quart. J. Math. Oxford Ser. (2) 26 (1975), 275-278.

7. J. Arkin, V. E. Hoggatt and E. G. Strauss, On Euler's solution of a problem of Diophantus, Fibonacci Quart. 17 (1979), 333-339.

8. A. Baker and H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, Quart. J. Math. Oxford Ser. (2) 20 (1969), 129-137.

9. K. S. Kedlaya, Solving constrained Pell equations, Math. Comp. 67 (1998), 833-842.

10. A. Dujella, The problem of the extension of a parametric family of Diophantine triples, Publ. Math. Debrecen 51 (1997), 311-322.

11. A. Dujella and A. Pethoe, A generalization of a theorem of Baker and Davenport, Quart. J. Math. Oxford Ser. (2), 49 (1998), 291-306.

12. Y. Fujita, The extensibility of Diophantine pairs $\{k-1, k+1\}$, J. Number Theory 128 (2008), 322-353.

13. A. Dujella, An absolute bound for the size of Diophantine m-tuples, J. Number Theory 89 (2001), 126-150.

14. A. Dujella, There are only finitely many Diophantine quintuples, J. Reine Angew. Math. 566 (2004), 183-214.

15. A. Filipin, Y. Fujita, The number of Diophantine quintuples II, Publ. Math. Debrecen 82 (2013), 293-308.

16. F. Luca and L. Szalay, Lucas Diophantine triples, Integers 9 (2009), #A35, 441-457.

17. M. Bliznac Trebješanin, A. Filipin, Nonexistence of D(4)-quintuples, J. Number Theory 194 (2019), 170-217.

18. F. Luca, On shifted products which are powers, Glas. Mat. Ser. III 40 (2005), 13-20.

19. A. Kihel and O. Kihel, Sets in which the product of any k elements increased by t is a kth-power, Fibonacci Quart. 39 (2001), 98-100.

20. A. Dujella & A. Jurasic, On the size of sets in a polynomial variant of a problem of Diophantus, Int. J. Number Theory 6 (2010), 1449-1471.

21. V. E. Hoggatt and G. E. Bergum, A problem of Fermat and the Fibonacci sequence, Fibonacci Quart. 15 (1977), 323-330.