

Some polynomial formulas for Diophantine quadruples

Andrej Dujella

The Greek mathematician Diophantus of Alexandria studied the following problem: Find four (positive rational) numbers such that the product of any two of them increased by 1 is a perfect square. He obtained the following solution: $\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}$ (see [4]).

Fermat obtained four positive integers satisfying the condition of the problem above: 1, 3, 8, 120. For example, $3 \cdot 120 + 1 = 19^2$. Later, Davenport and Baker [3] showed that if d is a positive integer such that the set $\{1, 3, 8, d\}$ has the property of Diophantus, then d has to be 120.

There are two direct generalizations of the set $\{1, 3, 8, 120\}$: the sets

$$\{n, n+2, 4n+4, 4(n+1)(2n+1)(2n+3)\}, \quad (1)$$

$$\{F_{2n}, F_{2n+2}, F_{2n+4}, 4F_{2n+1}F_{2n+2}F_{2n+3}\} \quad (2)$$

have the property of Diophantus for all positive integers n (see [9], [8]). For $n = 1$ we get the Fermat's solution. In [7] it was proved that these sets are two special cases of more general fact. Let the sequence (g_n) be defined as:

$$g_0 = 0, \quad g_1 = 1, \quad g_n = pg_{n-1} - g_{n-2}, \quad n \geq 2,$$

where $p \geq 2$ is an integer. Then the sets

$$\{g_n, g_{n+2}, (p \pm 2)g_{n+1}, 4g_{n+1}[(p \pm 2)g_{n+1}^2 \mp 1]\}$$

have the property of Diophantus. For $p = 2$ we get the set (1), and for $p = 3$ we get the set (2).

Let us now consider the more general problem.

Definition 1 Let n be an integer. A set of positive integers $\{a_1, a_2, \dots, a_m\}$ is said to have *the property of Diophantus of order n* , symbolically $D(n)$, if the product of its any two distinct elements increased by n is a perfect square. Such a set is called a *Diophantine m -tuple*.

In [5], the problem of the existence of the Diophantine quadruples with the property $D(n)$ was considered for an arbitrary integer n . The main results can be divided in the three groups.

1° If n is a perfect square then there exists an infinite number of Diophantine quadruples with the property $D(n)$. Precisely, for any set $\{a, b\}$ with the property

$D(n)$, where ab is not a perfect square, there exists an infinite number of Diophantine quadruples of the form $\{a, b, c, d\}$ with the property $D(n)$. There are also some explicit formulas for Diophantine quadruples with the property $D(l^2)$ (see [7]). For example: $\{1, l^4 - 3l^2 + 1, l^2(l^2 - 1), 4l^2(l^2 - 1)(l^2 - 2)\}$.

2° If n is an integer of the form $n = 4k + 2$, $k \in \mathbf{Z}$, then there does not exist Diophantine quadruple with the property $D(n)$ (see also [2]).

3° If $n \not\equiv 2 \pmod{4}$ and $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$ then there exists at least one Diophantine quadruple with the property $D(n)$ and if $n \notin S \cup T$, where $T = \{-15, -12, -7, 7, 13, 15, 21, 24, 28, 32, 48, 60, 84\}$, then there exist at least two different Diophantine quadruples with the property $D(n)$.

The results from the third group are proved by considering the following cases:

$$n = 4k + 3, \quad n = 8k + 1, \quad n = 8k + 5, \quad n = 8k, \quad n = 16k + 4, \quad n = 16k + 12.$$

In any of this cases, we can find two sets with the property $D(n)$ consisted of the four polynomials in k with integral coefficients. For example, the sets

$$\{1, k^2 - 2k + 2, k^2 + 1, 4k^2 - 4k - 3\}, \quad (3)$$

$$\{1, 9k^2 + 8k + 1, 9k^2 + 14k + 6, 36k^2 + 44k + 13\} \quad (4)$$

have the property $D(4k + 3)$. The elements from the sets S and T are exceptions because we can get the sets with nonpositive or equal elements for some values of k .

We will try now to describe how we can systematically find sets like (3) and (4).

For a polynomial P , the set of polynomials is said to have the property $D(P)$ if the product of any two its distinct elements increased by P is a square of a certain polynomial with a integral coefficients. In application of this formulas it is necessary (see [5]) to additionally discuss the problem for which parameters Diophantine quadruples, i. e. four different positive integers, are obtained.

The idea is similar to the original solution of Diophantus: $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$. Namely, his set is of the form

$$\{x, x + 2, 4x + 4, 9x + 6\}.$$

Product of any two distinct elements of this set, except second and fourth, increased by 1 is a square of a linear polynomial. So, it is sufficient to find a rational number x satisfying the equation $(x + 2)(9x + 6) + 1 = y^2$. Diophantus found one solution: $x = \frac{1}{16}$ (see [4]).

We will deal with the similar idea. Let $\{a, b\}$ be an arbitrary pair with the property $D(n)$, for an integer n . It means that

$$ab + n = x^2. \quad (5)$$

It is easy to check that the set $\{a, b, a + b + 2x\}$ also has the property $D(n)$. Indeed,

$$\begin{aligned} a(a + b + 2x) + n &= (a + x)^2, \\ b(a + b + 2x) + n &= (b + x)^2. \end{aligned}$$

Applying this construction to the Diophantine pair $\{b, a + b + 2x\}$ we get the set $\{b, a + b + 2x, a + 4b + 4x\}$. Therefore, the set

$$\{a, b, a + b + 2x, a + 4b + 4x\} \quad (6)$$

has the property $D(n)$ iff the product of its first and fourth element increased by n is a perfect square, i. e. iff it holds:

$$a(a + 4b + 4x) + n = y^2. \quad (7)$$

We will try to solve this equation using as less as possible restrictions on number n . We have: $a^2 + (4x^2 - 4n) + 4ax + n = y^2$, and

$$3n = (a + 2x - y)(a + 2x + y).$$

Let us consider two following cases:

$$\begin{aligned} 1) \quad & a + 2x - y = 3 \\ & a + 2x + y = n \end{aligned}$$

From this, $n = 2a + 4x - 3$ and from (5) it follows: $a(b + 2) = (x - 1)(x - 3)$.

Putting $x = ak + 1$ we get $b = ak^2 - 2k - 2$, $n = 2a(2k + 1) + 1$. Hence, we get the set

$$\{a, ak^2 - 2k - 2, a(k + 1)^2 - 2k, a(2k + 1)^2 - 8k - 4\} \quad (8)$$

with the property $D(2a(2k + 1) + 1)$. Putting $a = 1$ in (8) we get the set (3) with the property $D(4k + 1)$. For $a = 2$ we get the set with the property $D(8k + 5)$ and for $a = 4$, by substitution $k' = 2k + 1$, we get the set with the property $D(8k' + 1)$. Multiplying all elements of the set (8) by 2, putting $m = \frac{1}{2}$ and by substitution $k' = k + 1$, we get the set with the property $D(8k')$. Also, putting $m = 2$ and substituting $k' = 2k + 1$ we get the set with the property $D(16k' + 4)$. Finally, we get the set with the property $D(16k + 12)$ by multiplying all elements of the set (3) by 2.

Putting $x = ak + 3$, we get $b = ak^2 + 2k - 2$ and $n = 2a(2k + 1) + 9$. Hence, the set

$$\{a, ak^2 + 2k - 2, a(k + 1)^2 + 2k + 4, a(2k + 1)^2 + 8k + 4\} \quad (9)$$

has the property $D(2a(2k + 1) + 9)$. Note that the formulas obtained by putting $a = 1$ in (8) and (9) are equivalent.

$$\begin{aligned} 2) \quad & a + 2x - y = 1 \\ & a + 2x + y = 3n \end{aligned}$$

From this, $3n = 2a + 4x - 1$ and it follows from (5) that $a(3b + 2) = (3x - 1)(x - 1)$.

Let us put $x = am + 1$. Now, from $3b + 2 = m(3x - 1)$ we conclude that m is of the form $m = 3k + 1$. Using that, we get $b = a(3k + 1)^2 + 2k$, $n = 2a(2k + 1) + 1$ and the set

$$\{a, a(3k + 1)^2 + 2k, a(3k + 2)^2 + 2k + 2, 9a(2k + 1)^2 + 8k + 4\} \quad (10)$$

has the property $D(2a(2k+1)+1)$. For $a=1$, we get the set (4) with the property $D(4k+3)$.

Putting $3x = al + 1$, we have $b = \frac{1}{9}(al^2 - 2l - 6)$ and we get the formula for the Diophantine quadruples with the property $D(\frac{1}{9}(2a(2l+3)+1))$. For $a=1$ and $l=9k+5$, the same quadruple is obtained as quadruple obtained by putting $a=1$ in (10).

Let us now discuss the conditions if b and n are required to be the integers. From $l(al-2) \equiv 6 \pmod{9}$ and $4al+6a \equiv -1 \pmod{9}$ we have that $a \equiv l \not\equiv 0 \pmod{3}$. Putting $l=3k-2$ and $a=3d-1$ we get that $4k-d \equiv 1 \pmod{3}$. Finally, putting $d=4k-1+3m$ we obtain the set

$$\{9m+4(3k-1), (3k-2)^2m+2(k-1)(6k^2-4k+1), (3k+1)^2m+2k(6k^2+2k-1), \\ (6k-1)^2m+4k(2k-1)(6k-1)\} \quad (11)$$

with the property $D(2m(6k-1)+(4k-1)^2)$.

Choosing $l=3k-1$ instead $l=3k-2$ is equivalent to the change of the sign of k and m in the formula (11).

Summarizing the results obtained by examining the set (6) we have:

Theorem 1 *The sets*

$$\{m, mk^2 - 2k - 2, m(k+1)^2 - 2k, m(2k+1)^2 - 8k - 4\}, \\ \{m, m(3k+1)^2 + 2k, m(3k+2)^2 + 2k + 2, 9m(2k+1)^2 + 8k + 4\}$$

have the property $D(2m(2k+1)+1)$, the set

$$\{m, mk^2 + 2k - 2, m(k+1)^2 + 2k + 4, m(2k+1)^2 + 8k + 4\}$$

has the property $D(2m(2k+1)+9)$ and the set

$$\{9m+4(3k-1), (3k-2)^2m+2(k-1)(6k^2-4k+1), (3k+1)^2m+2k(6k^2+2k-1), \\ (6k-1)^2m+4k(2k-1)(6k-1)\}$$

has the property $D(2m(6k-1)+(4k-1)^2)$.

The similar idea can be applied to the set

$$\{a, b, a+b+2x, a+b-2x\}. \quad (12)$$

This set has the property $D(n)$ if and only if the product of its third and fourth element increased by n is a perfect square:

$$(a+b+2x)(a+b-2x)+n=y^2.$$

Hence, $3n = (b-a-y)(b-a+y)$. Again, we are going to discuss two different cases:

$$\begin{aligned} 1) \quad & b-a-y=3 \\ & b-a+y=n \end{aligned}$$

From this, $n = 2b - 2a - 3$ and from (5) it follows: $(a + 2)(b - 2) = (x - 1)(x + 1)$.

Putting $x = (a + 2)k + 1$ we get $b = ak^2 + 2(k^2 + k + 1)$ and $n = 2a(k^2 - 1) + (2k + 1)^2$. Therefore, we have the set

$$\{a, ak^2 + 2(k^2 + k + 1), a(k - 1)^2 + 2k(k - 1), a(k + 1)^2 + 2(k + 1)(k + 2)\} \quad (13)$$

with the property $D(2a(k^2 - 1) + (2k + 1)^2)$.

For $x = (a + 2)k - 1$, we get the equivalent result. Namely, we can get the obtained Diophantine quadruple by substituting $k' = -k$ in (13).

$$\begin{aligned} 2) \quad & b - a - y = 1 \\ & b - a + y = 3n \end{aligned}$$

Now, $3n = 2b - 2a - 1$ and, from (5), it follows: $(3a + 2)(3b - 2) = (3x - 1)(3x + 1)$.

Let us put $3x = (3a + 2)m + 1$. As $3b = m[(3a + 2)m + 2] + 2$, we conclude that m has to be of the form $m = 3k + 1$. Putting that in the formula, we get the set

$$\{a, a(3k + 1)^2 + 2(3k^2 + 3k + 1), a(3k + 2)^2 + 2(k + 1)(3k + 2), 9ak^2 + 2k(3k + 1)\} \quad (14)$$

with the property $D(2ak(3k + 2) + (2k + 1)^2)$.

For $3x = (3a + 2)k - 1$, the Diophantine quadruple equivalent to the (14) is obtained. We have thus proved

Theorem 2 *The set*

$$\{m, mk^2 + 2(k^2 + k + 1), m(k - 1)^2 + 2k(k - 1), m(k + 1)^2 + 2(k + 1)(k + 2)\}$$

has the property $D(2m(k^2 - 1) + (2k + 1)^2)$ and the set

$$\{m, m(3k + 1)^2 + 2(3k^2 + 3k + 1), m(3k + 2)^2 + 2(k + 1)(3k + 2), 9mk^2 + 2k(3k + 1)\}$$

has the property $D(2mk(3k + 2) + (2k + 1)^2)$.

Applying any formula from the Theorem 1 and 2 to the particular value of k gives the formula for the Diophantine quadruples with the property $D(n)$, where n is linear polynomial in m . Moreover, all elements of the quadruples are linear polynomials. For example, putting $k = 1$ in (11) gives the set $\{m, 9m + 8, 16m + 14, 25m + 20\}$ with the property $D(10m + 9)$. The question is which linear polynomials $am + b$ allow formulas of this type. Partial answer is given by the following theorem from [5].

Theorem 3 *If the set of polynomials $\{a_i m + b_i : i = 1, 2, 3, 4\}$ has the property $D(am + b)$, where a, b, a_i, b_i are the integers such that $\gcd(a_1, a_2, a_3, a_4, a) = \gcd(a, b) = 1$, then a is even and b is a quadratic residue modulo a .*

It was proved by Arkin and Bergum [1] that the set

$$\left\{ \frac{F_{12p} - F_{12r}}{4}, 9F_{12p} - F_{12r}, \frac{25F_{12p} - 9F_{12r}}{16}, \frac{49F_{12p} - F_{12r}}{16} \right\}$$

has the property $D(F_{12p}F_{12r})$. This result is the direct consequence of the fact that the set $\{4m, 144m + 8, 25m + 1, 49m + 3\}$ has the property $D(16m + 1)$.

It is shown in [6] how the similar result can be obtained when there is a set $\{a_i m + b_i : i = 1, 2, 3, 4\}$ with the property $D(am + b)$, where a, b, a_i, b_i are the integers. Namely, if we denote the index of the least Fibonacci number divisible by a with $Z(a)$, then the set

$$\left\{ \frac{a_i F_{Z(a)p} + (ab_i - a_i b) F_{Z(a)r}}{a} : i = 1, 2, 3, 4 \right\}$$

as the property $D(F_{Z(a)p}F_{Z(a)r})$.

References

- [1] J. Arkin and G. E. Bergum, *More on the problem of Diophantus*, in: *Applications of Fibonacci Numbers*, A. N. Philippou, A. F. Horadam and G. E. Bergum (eds.), Kluwer, Dordrecht, 1988, 177-181.
- [2] E. Brown, *Sets in which $xy + k$ is always a square*, Mathematics of Computation 45 (1985), 613-620.
- [3] H. Davenport and A. Baker, *The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$* , Quart. J. Math. Oxford Ser. (2) 20 (1969), 129-137.
- [4] Diofant Aleksandriiskii, *Arifmetika i kniga o mnogougol'nyh chislakh*, Nauka, Moscow, 1974.
- [5] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arithmetica 65 (1) (1993), 15-27.
- [6] A. Dujella, *Diophantine quadruples for squares of Fibonacci and Lucas numbers*, Portugaliae Mathematica 52 (3) (1995), 305-318.
- [7] A. Dujella, *Generalized Fibonacci numbers and the problem of Diophantus*, accepted for publication in The Fibonacci Quarterly.
- [8] V. E. Hoggatt and G. E. Bergum, *A problem of Fermat and the Fibonacci sequence*, The Fibonacci Quarterly 15 (1977), 323-330.
- [9] B. W. Jones, *A variation on a problem of Davenport and Diophantus*, Quart. J. Math. Oxford Ser. (2) 27 (1976), 349-353.

Andrej Dujella

Department of Mathematics, University of Zagreb

Bijenička cesta 30

10000 Zagreb CROATIA

E-mail: duje@math.hr