Conjectures and results on the size and number of Diophantine tuples

Andrej Dujella

Department of Mathematics, University of Zagreb
Bijenička cesta 30, 10000 Zagreb, CROATIA
E-mail: duje@math.hr
URL : http://web.math.hr/~duje/

Abstract

The problem of the construction of Diophantine m-tuples, i.e. sets with the property that the product of any two of its distinct elements is one less then a square, has a very long history. In this survey, we describe several conjectures and recent results concerning Diophantine m-tuples and their generalizations.

1 Diophantine quintuple conjecture

A set of m positive integers is called a Diophantine m-tuple if the product of its any two distinct elements increased by 1 is a perfect square. Diophantus himself found a set of four positive rationals with this property:

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}.$$

However, the first Diophantine quadruple, the set $\{1, 3, 8, 120\}$, was found by Fermat. Euler found an infinite family of 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's set (see [5, 6, 26]). Recently, Gibbs [24] found several examples of sets of six positive rationals with the property of Diophantus. The first one was

$$\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}.$$

A folklore conjecture is that there does not exist a Diophantine quintuple. The first important result concerning this conjecture was proved in 1969 by Baker and Davenport [2]. They proved that if d is a positive integer such that

$\{1, 3, 8, d\}$ forms a Diophantine quadruple, then $d = 120$. This problem was stated in 1967 by Gardner [23] (see also [27]). Furthemore, in 1998, in the joint work with Attila Pethő [17] we proved that the pair $\{1, 3\}$ cannot be extended to a Diophantine quintuple.

In 1979, Arkin, Hoggatt and Strauss [1] 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 integers. Define

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

Then $\{a, b, c, d_+\}$ is a Diophantine quadruple. A stronger version of the Diophantine quintuple conjecture states that if $\{a, b, c, d\}$ is a Diophantine quadruple and $d > \max\{a, b, c\}$, then $d = d_+$. Diophantine quadruples of this form are called regular.

In 2004, we proved that there does not exist a Diophantine sextuple and there are only finitely many Diophantine quintuples (see [10]). However, the bounds for the size of the elements of a (hypothetical) Diophantine quintuple are huge (largest element is less than $10^{10^{26}}$), so the remaining cases cannot be checked on a computer.

Recently, Fujita [22] proved that if $\{a, b, c, d, e\}$ $(a < b < c < d < e)$ is a Diophantine quintuple, then $\{a, b, c, d\}$ is a regular Diophantine quadruple. Thus, in order to prove the Diophantine quintuple conjecture, it remains to prove that a regular Diophantine quadruple cannot be extended to a quintuple. Such result is known to be true for several parametric families of regular Diophantine quadruples, e.g. $\{k - 1, k + 1, 4k, 16k^3 - 4k\}$. Moreover, Fujita [21] proved that the pair $\{k-1, k+1\}$ (for $k \geq 2$) cannot be extended to a Diophantine quintuple, and his results, together with our joint work with Yann Bugeaud and Maurice Mignotte [4], show that all Diophantine quadruples of the form $\{k-1, k+1, c, d\}$ are regular.

2 The existence of Diophantine quadruples with the property $D(n)$

A natural generalization of the original problem of Diophantus and Fermat is to replace number 1, in the definition of Diophantine m-tuples, by an arbitrary integer n. A set of m positive integers $\{a_1, a_2, \ldots, a_m\}$ is said to have the property $D(n)$ if $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$. Such a set is called a Diophantine m-tuple with the property $D(n)$ (or $D(n)$-m-tuple, or P_n-set of size m).

Several authors considered the problem of the existence of Diophantine quadruples with the property $D(n)$. This problem is now almost completely solved. In 1985, Brown [3] (see also [25, 28]) gave the first part of the answer by showing that if n is an integer of the form $n = 4k+2$, then there does not exist a Diophantine quadruple with the property $D(n)$. In 1993, we were able to prove that if $n \not\equiv 2 \pmod 4$ and $n \notin S = \{-4, -3, -1, 3, 5, 12, 20\}$, then there exists at least one Diophantine quadruple with the property $D(n)$ (see [7]). The conjecture is that for $n \in S$ there does not exist a Diophantine quadruple with the property $D(n)$. It is interesting to observe that the integers $4k+2$ are exactly those integers which are not representable as differences of the squares of two integers. It seems that this is not just a coincidence. Namely, analogous results, which show strong connection between the existence of $D(n)$-quadruples and the representability as a difference of two squares, also hold for integers in some quadratic fields (see [8, 15, 19, 20]).

It is clear that if $n = m^2$ is a perfect square, than there exist infinitely many $D(m^2)$-quadruples. Namely, Euler's result mentioned above shows that there are infinitely many $D(1)$-quadruples, and multiplying their elements by m we obtain $D(m^2)$-quadruples. We state the following conjecture: if n is not a perfect square, then there exist only finitely many $D(n)$-quadruples. As we already mentioned, it is easy to verify the conjecture in case $n \equiv 2 \pmod 4$ (then there does not exist a $D(n)$-quadruple). In the recent joint work with Clemens Fuchs and Alan Filipin, we have proved this conjecture in cases $n = -1$ and $n = -4$ (see [14, 16]). Perhaps some support to this conjecture may come from considering the number of $D(n)$-triples in given range. Let

$$D_m(n; N) = |\,\{D \subseteq \{1, 2, \dots, N\} \,:\, D \text{ is a } D(n)\text{-}m\text{-tuple }\}\,|.$$

In [12], we considered the case $n = 1$ and proved that $D_3(1; N) = \frac{3}{\pi^2} N \log N + O(N)$. In our forthcoming paper [18], we will show that $D_3(n; N) \sim C(n) N \log(N)$ if n is a perfect square, while $D_3(n; N) \sim C(n) N$ otherwise.

Concerning rational Diophantine m-tuples, it is expected that there exist an absolute upper bound for their size. Such a result will follow from the Lang conjecture on varieties of general type. Related problem is to find an upper bound M_n for the size of $D(n)$-tuples (for given non-zero integer n). Again, the Lang conjecture implies that there exist an absolute upper bound for M_n (independent on n). However, at present, the best known upper bounds are of the shape $M_n < c \log |n|$ (see [9, 11]). Recently, in our joint paper with Florian Luca [13], we were able to obtain an absolute upper bound for M_p, where p is a prime.

References

[1] J. Arkin, V. E. Hoggatt and E. G. Strauss, *On Euler's solution of a problem of Diophantus*, Fibonacci Quart. **17**, 333–339 (1979).

[2] 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**, 129–137 (1969).

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

[4] Y. Bugeaud, A. Dujella and M. Mignotte, *On the family of Diophantine triples* $\{k-1, k+1, 16k^3-4k\}$, Glasgow Math. J. **49**, 333–344 (2007).

[5] L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Chelsea, New York, 1966, pp. 513–520.

[6] Diophantus of Alexandria, *Arithmetics and the Book of Polygonal Numbers*, (ed. I. G. Bashmakova), Nauka, Moscow, 1974 (in Russian), pp. 103–104, 232.

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

[8] A. Dujella, *The problem of Diophantus and Davenport for Gaussian integers*, Glas. Mat. Ser. III **32**, 1–10 (1997).

[9] A. Dujella, *On the size of Diophantine m-tuples*, Math. Proc. Cambridge Philos. Soc. **132**, 23–33 (2002).

[10] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566**, 183–214 (2004).

[11] A. Dujella, *Bounds for the size of sets with the property $D(n)$*, Glas. Mat. Ser. III **39**, 199–205 (2004).

[12] A. Dujella, *On the number of Diophantine m-tuples*, Ramanujan J., to appear.

[13] A. Dujella and F. Luca, *Diophantine m-tuples for primes*, Intern. Math. Research Notices **47**, 2913–2940 (2005).

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

[15] A. Dujella and Z. Franušić, *On differences of two squares in some quadratic fields*, Rocky Mountain J. Math. **37**, 429–453 (2007).

[16] A. Dujella and C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. **71**, 33–52 (2005).

[17] A. Dujella and A. Pethő, *Generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) **49**, 291–306 (1998).

[18] A. Dujella and A. Pethő, *Asymptotic estimates for the number of Diophantine pairs and triples*, in preparation.

[19] Z. Franušić, *Diophantine quadruples in* $\mathbb{Z}[\sqrt{4k+3}]$, Ramanujan J., to appear.

[20] Z. Franušić, *A Diophantine problem in* $\mathbb{Z}[(1+\sqrt{d})/2]$, Studia Sci. Math. Hungar., to appear.

[21] Y. Fujita, *The extensibility of Diophantine pairs* $\{k-1, k+1\}$, J. Number Theory, to appear.

[22] Y. Fujita, *Any Diophantine quintuple contains a regular Diophantine quadruple*, preprint.

[23] M. Gardner, *Mathematical divertions*, Scientific American **216**, 124 (1967).

[24] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41**, 195–203 (2006).

[25] H. Gupta and K. Singh, *On* k*-triad sequences*, Internat. J. Math. Math. Sci. **5**, 799–804 (1985).

[26] T. L. Heath, *Diophantus of Alexandria. A Study of the History of Greek Algebra*, Powell's Bookstore, Chicago; Martino Publishing, Mansfield Center, 2003. pp. 177–181.

[27] J. H. van Lint, *On a set of diophantine equations*, T. H.-Report 68 – WSK-03, Technological University Eindhoven, 1968.

[28] S. P. Mohanty and A. M. S. Ramasamy, *On* $P_{r,k}$ *sequences*, Fibonacci Quart. **23**, 36–44 (1985).