

# Diophantine $m$ -tuples and generalizations

Andrej Dujella

Department of Mathematics  
University of Zagreb, Croatia

e-mail: [duje@math.hr](mailto:duje@math.hr)

URL: <http://web.math.pmf.unizg.hr/~duje/>

**Diophantus:** Find four numbers such that the product of any two of them, increased by 1, is a perfect square:

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

**Fermat:**  $\{1, 3, 8, 120\}$

$$\begin{aligned} 1 \cdot 3 + 1 &= 2^2, & 3 \cdot 8 + 1 &= 5^2, \\ 1 \cdot 8 + 1 &= 3^2, & 3 \cdot 120 + 1 &= 19^2, \\ 1 \cdot 120 + 1 &= 11^2, & 8 \cdot 120 + 1 &= 31^2. \end{aligned}$$

**Euler:**  $\{1, 3, 8, 120, \frac{777480}{8288641}\}$

$$ab + 1 = r^2 \mapsto \{a, b, a + b + 2r, 4r(a + r)(b + r)\}$$

**Gibbs (1999):**  $\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}$

**Dujella (2009):**  $\left\{\frac{27}{35}, -\frac{35}{36}, -\frac{352}{315}, \frac{1007}{1260}, -\frac{5600}{4489}, \frac{72765}{106276}\right\}$

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

**Question:** How large such sets can be?

**Conjecture 1:** There does not exist a Diophantine quintuple.

**Baker & Davenport (1969):**

$$\{1, 3, 8, d\} \Rightarrow d = 120$$

(problem raised by Gardner (1967), van Lint (1968))

**Arkin, Hoggatt & Strauss (1978):** Let

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2$$

and define

$$d_{+,-} = a + b + c + 2abc \pm 2rst.$$

Then  $\{a, b, c, d_{+,-}\}$  is a Diophantine quadruple  
(if  $d_- \neq 0$ ).

**Conjecture 2:** If  $\{a, b, c, d\}$  is a Diophantine quadruple,  
then  $d = d_+$  or  $d = d_-$ , i.e. all Diophantine quadruples  
satisfy

$$(a - b - c + d)^2 = 4(ad + 1)(bc + 1).$$

Such quadruples are called *regular*.

**D. & Fuchs (2004):** All Diophantine quadruples in  $\mathbb{Z}[X]$  are regular.

**D. & Jurasić (2010):** In  $\mathbb{Q}(\sqrt{-3})[X]$ , the Diophantine quadruple

$$\left\{ \frac{\sqrt{-3}}{2}, -\frac{2\sqrt{-3}}{3}(X^2 - 1), \frac{-3 + \sqrt{-3}}{3}X^2 + \frac{2\sqrt{-3}}{3}, \frac{3 + \sqrt{-3}}{3}X^2 + \frac{2\sqrt{-3}}{3} \right\}$$

is not regular.

**D. (1997):**  $\{k - 1, k + 1, 4k, d\} \Rightarrow d = 16k^3 - 4k$

**D. & Pethő (1998):**  $\{1, 3\}$  cannot be extended to a Diophantine quintuple

**Fujita (2008):**  $\{k - 1, k + 1\}$  cannot be extended to a Diophantine quintuple

**Bugeaud, D. & Mignotte (2007):**

$\{k - 1, k + 1, 16k^3 - 4k, d\} \Rightarrow$   
 $d = 4k$  or  $d = 64k^5 - 48k^3 + 8k$

**D. (2004):** There does not exist a Diophantine sextuple.  
There are only finitely many Diophantine quintuples.

$$\max\{a, b, c, d, e\} < 10^{10^{26}}$$

**Fujita (2009):** If  $\{a, b, c, d, e\}$ , with  $a < b < c < d < e$ , is a Diophantine quintuple, then  $\{a, b, c, d\}$  is a regular Diophantine quadruple.



Extending the Diophantine triple  $\{a, b, c\}$ ,  $a < b < c$ , to a Diophantine quadruple  $\{a, b, c, d\}$ :

$$ad + 1 = x^2, \quad bd + 1 = y^2, \quad cd + 1 = z^2.$$

**System of simultaneous Pellian equations:**

$$cx^2 - az^2 = c - a, \quad cy^2 - bz^2 = c - b.$$

**Binary recursive sequences:**

finitely many equations of the form  $v_m = w_n$ .

**Linear forms in three logarithms:**

$$v_m \approx \alpha\beta^m, \quad w_n \approx \gamma\delta^n \Rightarrow \\ m \log \beta - n \log \delta + \log \frac{\alpha}{\gamma} \approx 0$$

Baker's theory gives upper bounds for  $m, n$  (logarithmic functions in  $c$ ).

### **Simultaneous Diophantine approximations:**

$\frac{x}{z}$  and  $\frac{y}{z}$  are good rational approximations to  $\sqrt{\frac{a}{c}}$  and  $\sqrt{\frac{b}{c}}$ , resp.

$\frac{bsx}{abz}$  and  $\frac{aty}{abz}$  are good rational approximations to  $\frac{s}{a}\sqrt{\frac{a}{c}} = \sqrt{1 + \frac{b}{abc}}$  and  $\frac{t}{b}\sqrt{\frac{b}{c}} = \sqrt{1 + \frac{a}{abc}}$ , resp.

If  $c$  is large compared to  $b$  (say  $c > b^6$ ), then hypergeometric method gives (very good) upper bounds for  $x, y, z$ .

### **Congruence method (D. & Pethő):**

$$v_m \equiv w_n \pmod{c^2}$$

If  $m, n$  are small (compared with  $c$ ), then  $\equiv$  can be replaced by  $=$ , and this (hopefully) leads to a contradiction (if  $m, n > 2$ ).

Therefore, we obtain lower bounds for  $m, n$  (small powers of  $c$ , e.g.  $c^{0.04}$ ).

**Conclusion:** Contradiction for large  $c$ .

If  $\{k-1, k+1, c\}$  is a Diophantine triple, then  $c = c_\nu$ , where

$$c_1 = 4k, \quad c_2 = 16k^3 - 4k, \quad c_3 = 64k^5 - 48k^3 + 8k, \dots$$

For  $c_\nu$ ,  $\nu \geq 3$ , gap is large enough for the application of results on simultaneous Diophantine approximations – **Fujita (2008)**.

The case  $c_1$  leads to simultaneous approximations to the numbers  $\sqrt{1 - \frac{1}{k}}$  and  $\sqrt{1 + \frac{1}{k}}$  (a result by **Rickert (1993)**) – **D. (1997)**.

For  $c_2$  – **Bugeaud, D. & Mignotte (2007)**:

Improved congruence method:

Combination of congruences mod  $4k(k-1)$  and mod  $c_2^2$   
gives  $m > 4.9k^{1.5}$  (if  $m > 2$ ).

Recent results on linear forms in three logarithms:

by **Matveev (2000)**:  $k < 3.8 \cdot 10^{10}$ ;

by **Mignotte (2007)**:  $k < 5.4 \cdot 10^8$ .

**Baker-Davenport** reduction method:

Starting with  $m \leq 3.6 \cdot 10^{16}$ , we obtain  $m \leq 2$ .

**Bo He, Togbé, Filipin (2009,2012):**

$$\{k, A^2k + 2A, (A + 1)^2k + 2(A + 1)\}$$

extends uniquely to a Diophantine quadruple if

$$1 \leq A \leq 22 \text{ or } A \geq 51767$$

(using linear forms in *two* logarithms)

Let  $\{a, b, c\}$  be a Diophantine triple. Consider the elliptic curve

$$E : y^2 = (ax + 1)(bx + 1)(cx + 1).$$

Rational points  $P = [0, 1]$ ,  $Q = [1/abc, rst/abc]$  satisfy  $x(P \mp Q) = d_{+,-}$ .

**Conjecture 3:** All integer points on  $E$  are:  $[0, \pm 1]$ ,  
 $[d_+, \pm(at + rs)(bs + rt)(cr + st)]$ ,  
 $[d_-, \pm(at - rs)(bs - rt)(cr - st)]$ ,  
and also  $[-1, 0]$  if  $1 \in \{a, b, c\}$ .

**D. (2000):** Conjecture is true for elliptic curves

$$E_k : y^2 = ((k-1)x+1)((k+1)x+1)(4kx+1),$$

under assumption that  $\text{rank } E_k(\mathbb{Q}) = 1$  (also for two subfamilies of rank 2 and one subfamily of rank 3). Furthermore, it is true for all  $k$ ,  $2 \leq k \leq 1000$  (extended to  $k \leq 5000$  by **Najman (2010)**).

The condition  $\text{rank } E_k(\mathbb{Q}) = 1$  is not unrealistic since  $\text{rank } E(\mathbb{Q}(k)) = 1$ .



**D. & Pethő (2000)**: Conjecture is true for elliptic curves

$$E'_k : y^2 = (x + 1)(3x + 1)(c_k x + 1),$$

where  $\{1, 3, c_k\}$  is a Diophantine triple, i.e.

$$c_k = \frac{1}{6} \left( (2 + \sqrt{3})(7 + 4\sqrt{3})^k + (2 - \sqrt{3})(7 - 4\sqrt{3})^k - 4 \right),$$

under assumption that  $\text{rank } E'_k(\mathbb{Q}) = 2$ . Furthermore, it is true for all  $k$ ,  $1 \leq k \leq 40$ , with possible exceptions  $k = 23$  and  $k = 37$  (extended by **Jacobson & Williams (2002)** to  $k \leq 100$ , with the possible exception of  $k = 37$ , for which the result holds under the Extended Riemann Hypothesis).

Similar results for other families of Diophantine triples: **D. (2001)**, **Fujita (2007, 2008)**, **Najman (2009, 2010)**.

**Definition:** Let  $n$  be an integer. A set of  $m$  positive integers is called *a Diophantine  $m$ -tuple with the property  $D(n)$*  or simply  *$D(n)$ - $m$ -tuple* (or  $P_n$ -set of size  $m$ ), if the product of any two of them, increased by  $n$ , is a perfect square.

$$M_n = \sup\{\#D : D \text{ is a } D(n)\text{-tuple}\}$$

**Conjecture 4:** There exist a constant  $C$  such that  $M_n < C$  for all non-zero integers  $n$ .  
In particular, there does not exist a rational  $C$ -tuple.

**D. (2004):**  $4 \leq M_1 \leq 5$   
(implies directly  $4 \leq M_4 \leq 7$ )

**Filipin (2008):**  $4 \leq M_4 \leq 5$

**D. (2004):**  $M_n \leq 31$  if  $|n| \leq 400$   
 $M_n < 15.476 \cdot \log |n|$  if  $|n| > 400$

**D. & Luca (2005):**  $M_p < 2^{146}$  if  $p$  is a prime

**Brown, Gupta & Singh, Mohanty & Ramasamy (1985):**

If  $n \equiv 2 \pmod{4}$ , then  $M_n = 3$ .

**D. (1993):** If  $n \not\equiv 2 \pmod{4}$  and  $n \notin S_1 = \{-4, -3, -1, 3, 5, 8, 12, 20\}$ , then  $M_n \geq 4$ .

**Conjecture 5:** If  $n \in S_1$ , then  $M_n = 3$ .

**D. & Fuchs (2005):**  $3 \leq M_{-1} \leq 4$

**Remark:**  $n \equiv 2 \pmod{4}$  if and only if  $n$  is not representable as a difference of the squares of two integers.

**D. (1997), Franušić (2004, 2008):** Analogous results: 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.

**D., Filipin & Fuchs (2007):**

There are only finitely many  $D(-1)$ -quadruples.

If  $\{a, b, c, d\}$  is a  $D(-1)$ -quadruple, then  
 $\max\{a, b, c, d\} < 10^{10^{23}}$ .

**Conjecture 6:** If  $n$  is not a perfect square, then there exist only finitely many  $D(n)$ -quadruples.

**Euler:** There exist infinitely many  $D(1)$ -quadruples, and therefore infinitely many  $D(k^2)$ -quadruples.

**DFE** implies that the conjecture is true for  $n = -1$  and  $n = -4$  (note that all elements of a  $D(-4)$ -quadruple are even).

**D. (2000):** For any rational  $q$  there exist infinitely many rational  $D(q)$ -quadruples.

**Question:** For which rationals  $q$  there exist infinitely many rational  $D(q)$ -quintuples.

We may restrict our attention to square-free integers  $q$ , since by multiplying all elements of a  $D(q)$ - $m$ -tuple by  $r$  we get a  $D(qr^2)$ - $m$ -tuple.

**Euler:**  $q = 1$

**D. (2000):**  $q = -3$

$$\left\{ \frac{5}{4}, \frac{12}{5}, \frac{133}{5}, \frac{73}{20}, \frac{217}{20} \right\}$$

**D. (2002):**  $q = -1$

$$\left\{ 10, \frac{25}{8}, \frac{37}{10}, \frac{13}{40}, \frac{533}{40} \right\}$$

**D. & Fuchs (2012):** For infinitely many square-free integers  $q$  for which the elliptic curve

$$qy^2 = x^3 + 86x^2 + 825x$$

has positive rank (conjecturally the set of all such square-free integers has density  $\geq 1/2$ ).



$$a_i \cdot a_j + 1 = k\text{-th power} \quad k \geq 3 \text{ fixed}$$

Such a set is called *a  $k$ -th power Diophantine  $m$ -tuple*.

$\{2, 171, 25326\}$  is a third power Diophantine triple

$\{1352, 8539880, 9768370\}$  is a fourth power Diophantine triple

$$C(k) = \sup\{\#D : D \text{ is a } k\text{-th power D. tuple}\}$$

**Bugeaud & D. (2003):**  $C(3) \leq 7$ ,  $C(4) \leq 5$ ,  $C(k) \leq 4$   
for  $5 \leq k \leq 176$ ,  $C(k) \leq 3$  for  $k \geq 177$

$$a_i \cdot a_j + 1 = \text{perfect power}$$

Such a set is called *a Diophantine powerset*.

$D \subset \{1, 2, \dots, N\}$  such that  $ab + 1$  is a perfect power for all  $a \neq b$  in  $D$ .

**Gyarmati, Sárközy & Stewart (2002):**

$$\#D \leq 340 \frac{(\log N)^2}{\log \log N}$$

Improvements by **Bugeaud-Gyarmati (2004)**,  
**Dietmann-Elsholtz-Gyarmati-Simonovits (2005)**,  
**Luca (2005)**, **Gyarmati-Stewart (2007)**

**Stewart (2008):**  $\#D \ll (\log N)^{2/3} (\log \log N)^{1/3}$

**Luca (2005):** *abc-conjecture* implies that  $\#D$  is bounded by an absolute constant.

**D., Fuchs & Luca (2008):**

In  $\mathbb{Z}[X]$ ,  $\#D < 8 \cdot 10^5$ .

**D. & Jurasić (2010):**

In  $\mathbb{K}[X]$ , where  $\mathbb{K}$  is a field of characteristic 0,  $\#D < 2 \cdot 10^7$ .

Let  $D_m(N) =$   
 $\# \{D \subseteq \{1, 2, \dots, N\} : D \text{ is a Diophantine-}m\text{-tuple}\}.$

**D. (2008):**  $D_2(N) = \frac{6}{\pi^2} N \log N + O(N);$   
 $ab + 1 = r^2 \rightarrow r^2 \equiv 1 \pmod{b}$

$D_3(N) = \frac{3}{\pi^2} N \log N + O(N);$   
almost all triples are of form  $\{a, b, a + b + 2r\}$

$0.1608 \sqrt[3]{N} \log N < D_4(N) < 0.5354 \sqrt[3]{N} \log N$

### Martin & Sitar (2010):

$D_4(N) = C\sqrt[3]{N} \log N + O(\sqrt[3]{N}(\log N)^{2/3+\sqrt{2}/6}(\log \log N)^{5/12})$ , where

$$C = \frac{2^{4/3}}{3\Gamma(\frac{2}{3})^3} \approx 0.338285$$

almost all quadruples are on the form

$$\{a, b, a + b + 2r, 4r(a + r)(b + r)\};$$

Erdős-Turán inequality - discrepancy between the number of elements of a sequence that lie in a particular interval modulo 1 and the expected number;

equidistribution of solutions of polynomial congruences

### Fujita (2010): $D_5(N) < 10^{276}$

a fixed Diophantine triple  $\{a, b, c\}$  has at most 4 extensions to Diophantine quintuple  $\{a, b, c, d, e\}$  such that  $\max\{a, b, c\} < d < e$

$$a_i \cdot a_j + n = \text{perfect power}$$

**Bérczes, D., Hajdu & Luca (2011):**

The size of such sets cannot be bounded by an absolute constant.

More precisely, let  $x \geq e^{e^e}$ , and take  $K = \left\lfloor \left( \frac{\log \log x}{2 \log \log \log x} \right)^{1/3} \right\rfloor$ .

Then there exists a set  $\mathcal{A}_K = \{a_1, \dots, a_K\}$  with elements all in  $[1, x]$ , as well as an integer  $n_K$  also in  $[1, x]$ , such that  $a_i a_j + n_K = x_{ij}^{k_{ij}}$  for  $1 \leq i < j \leq K$  with some integers  $x_{ij}$ , where the exponents  $k_{ij}$  are the first  $\binom{K}{2}$  primes.

Assuming the *abc*-conjecture, the size of such sets can be bounded by a constant depending only on  $n$  (generalization of **Luca (2005)** for  $n = 1$ ).