Conjectures and results on the size and number of Diophantine tuples

Andrej Dujella

Department of Mathematics
University of Zagreb, Croatia
e-mail: `duje@math.hr`
URL: `http://web.math.hr/~duje/`

Diophantus: Find four (positive rational) 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: $\{1, 3, 8, 120, \frac{777480}{2879^2}\}$

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

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

Definition: A set $\{a_1, a_2, \ldots, a_m\}$ of m positive 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))

Arkin, Hoggatt & Strauss (1978): Let

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

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 are *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 (2008): 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.

Extending the Diophantine triple $\{a,b,c\}$ ($a \le b \le c$) 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:
$v_m \approx \alpha\beta^m$, $w_n \approx \gamma\delta^n \ \Rightarrow$
$m\log\beta - n\log\delta + \log\frac{\alpha}{\gamma} \approx 0$
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 (Bennett's result (1998)) gives (very good) upper bounds for x, y, z.

Congruence method:
$v_m \equiv w_n \pmod{c^2}$
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).

Conclusion: Contradiction for large c.

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 3: 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 4: 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, 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.

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 5: 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.

DFF implies that the conjecture is true for $n = -1$ and $n = -4$.

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

D. (2008): $D_3(1; N) = \frac{3}{\pi^2} N \log N + O(N)$;
$0.1608 \sqrt[3]{N} \log N < D_4(1; N) < 0.5354 \sqrt[3]{N} \log N$ for large N.

D. & Pethő (2008):
$D_3(n; N) \sim C(n) N \log(N)$ if n is a perfect square,
$D_3(n; N) \sim C(n) N$ otherwise.

D. (1993): If $n \not\equiv 2 \pmod 4$ and $n \not\in S_2$, where $S_2 = S_1 \cup \{-15, -12, -7, 7, 13, 15, 21, 24, 28, 32, 48, 60, 84\}$, then there exist at least two different $D(n)$-quadruples.

Conjecture 6: The set S_3 of all integers n, not of the form $4k+2$, with the property that there exist at most two different $D(n)$-quadruples is infinite.

D. (1998, 2008): Let n be an integer such that $n \equiv 3 \pmod 4$, $n \not\in \{-9, -1, 3, 7, 11\}$, and there exist at most two different $D(n)$-quadruples. Then $|n-1|/2$, $|n-9|/2$ and $|9n-1|/2$ are primes. Furthermore, either $|n|$ is prime or $n = pq$, where $p \equiv 3 \pmod 4$ and $q = p + 2$ are twin primes.

D. (1993): For an integer $k \notin \{-1, 0, 1, 2\}$, the sets
$\{1, k^2 - 2k - 2, k^2 + 1, 4k^2 - 4k - 3\}$ and
$\{1, 9k^2 + 8k + 1, 9k^2 + 14k + 6, 36k^2 + 44k + 13\}$
are two different $D(4k + 3)$-quadruples.

D. (2008): If $k \notin \{-1, 0\}$ is an integer, then
$\{1,\ 144k^4 + 216k^3 + 113k^2 + 20k + 1,$
$144k^4 + 360k^3 + 329k^2 + 134k + 22,$
$576k^4 + 1152k^3 + 848k^2 + 272k + 33\}$
is a $D((4k + 1)(4k + 3))$-quadruple.

Definition: A set S of m non-zero rationals is called *a strong Diophantine m-tuple* if $xy+1$ is a perfect square for all $x, y \in S$ (including $x = y$).

$$\left\{\frac{1976}{5607}, \frac{3780}{1691}, \frac{14596}{1197}\right\}$$

D. & Petričević: There exist infinitely many strong Diophantine triples.

Conjecture 7: There does nor exist a strong Diophantine quintuple.

Example:
"almost strong Diophantine quadruple"

$$\{a, b, c, d\}$$

such that a^2+1, b^2+1, c^2+1, d^2+1, $ab+1$, $ac+1$, $ad+1$, $bc+1$ and $bd+1$ are perfect squares, but $cd+1$ is not a perfect square:

$$\left\{\frac{140}{51}, \frac{2223}{30464}, \frac{278817}{33856}, \frac{3182740}{17661}\right\}$$

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

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

Conjecture 8: 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

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

under assumption that $\operatorname{rank} E_k(\mathbb{Q}) = 1$ (also for two subfamilies of rank 2 and one subfamily of rank 3). Furthermore, it is true for all k, $2 \leq k \leq 1000$. The condition $\operatorname{rank} E_k(\mathbb{Q}) = 1$ is not unrealistic since $\operatorname{rank} E(\mathbb{Q}(k)) = 1$.

Similar results for other families:
D.-Pethő (2000), D. (2001) and Fujita (2007, 2008).

Conjecture 9: For an integer r and a group $T \in \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}\}$ there exist a rational Diophantine triple $\{a, b, c\}$ such that the elliptic curve

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

has rank $\geq r$ and torsion group isomorphic to T.

D. (2007):

$\{3164/491, 10692/491, 302996685420/118370771\}$
$r = 9$ and $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\{-22552/5129, 5129/22552, -52463190/14458651\}$
$r = 7$ and $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

$\{39123/96976, 12947200/418209, 42427/1104\}$
$r = 4$ and $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

$\{145/408, -408/145, -145439/59160\}$
$r = 3$ and $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$