# A problem of Diophantus, Fermat and Euler and its generalizations

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.

**D. & Fuchs (2004):** Conjecture 2 is true in $\mathbb{Z}[X]$.

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:**
$v_m \approx \alpha\beta^m$, $w_n \approx \gamma\delta^n \Rightarrow$
$m \log \beta - n \log \delta + \log \frac{\alpha}{\gamma} \approx 0$
Baker's theory (Baker-Wüstholz, Matveev, Mignotte) 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 (Rickert, Bennett, Fujita, Jadrijević-Ziegler) gives (very good) upper bounds for $x, y, z$.

**Congruence method:**
$v_m \equiv w_n \pmod{f(c)}$, e.g. $f(c) = c^2$ (Dujella-Pethő)
If $m, n$ are small (compared with $c$), then $\equiv$ can be replaced by $=$, and this (usually) 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

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

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 $\sqrt{1 + \frac{1}{k}}$ (Rickert (1993)) – Dujella (1997).

For $c_2$, different approach is needed – Bugeaud, Dujella & 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:**

Matveev (2000):
contradiction for $k \geq 3.8 \cdot 10^{10}$;

Mignotte (2008):
contradiction for $k \geq 5.4 \cdot 10^{8}$.

**Baker-Davenport reduction method:**

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

**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: 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 $n = -4$ (note that all elements of a $D(-4)$-quadruple are even).

**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 (2008):** There exist infinitely many strong Diophantine triples.

**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 7:** 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 $k$, $2 \le k \le 1000$ ($k \le 5000$ Najman (2008)). 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)
(computation extended by Jacobson-Williams (2002) and Najman (2008)).

**Conjecture 8:** 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 $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

$\boxed{a_i \cdot a_j + 1 = k\text{-th-power}}$ $k \geq 3$ 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 $k \geq 177$

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

Such a set is called *a Diophantine powerset*.

$D \subset \{1, 2, \ldots, N\}$ 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 $\mathbb{Z}[X]$, $\#D < 8 \cdot 10^5$.