Four (and seven) squares from three numbers

Andrej Dujella

Department of Mathematics, Faculty of Science
University of Zagreb, Croatia
URL: `https://web.math.pmf.unizg.hr/~duje/`

Joint work with **László Szalay**, **Matija Kazalicki** *and* **Vinko Petričević**

Number Theory Seminar, Debrecen
May 22, 2026

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

Euler: $\{1, 3, 8, 120, \frac{777480}{8288641}\}$
(extension is unique – Stoll (2019))

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

Definition: A set $\{a_1, a_2, \ldots, a_m\}$ 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 $1 \leq i < j \leq m$.

Question: How large such sets can be?

Baker & Davenport (1969): $\{1, 3, 8, d\} \Rightarrow d = 120$ (problem raised by Denton (1957), Gardner (1967), van Lint (1968))

D. (2004): no Diophantine sextuples; only finitely many quintuples.

He, Togbé & Ziegler (2019): no Diophantine quintuples.

For rational Diophantine tuples, the situation is much more open. There is no known upper bound for the size of rational Diophantine tuples.

Euler: There are infinitely many rational Diophantine quintuples. Any pair $\{a, b\}$ such that $ab+1 = r^2$ can be extended to a quintuple.

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

D., Kazalicki, Mikić & Szikszai (2017); D. & Kazalicki (2017); D., Kazalicki & Petričević (2019,2021): There are infinitely many rational Diophantine sextuples.

No rational Diophantine septuple is known.

Kevin Brown (attributed to John Gowland) (1998): Find three integers such that all four of the quantities $ab+1$, $ac+1$, $bc+1$, $abc+1$ are distinct squares (equivalently, each of the numbers a, b, c must be greater than 1).

Problem appeared later on several internet forums and also in Section 14.5 of the book *Numbers* by Kevin Brown (2023).

Examples listed by Brown include

$$(5,7,24), \quad (8,45,91), \quad (8,105,171),$$
$$(3,133,176), \quad (11,105,184), \quad (20,84,186).$$

Question. Are there infinitely many such triples?

Kenta Takahashi (student of Takafumi Miyazaki) (2010):

A $D^{(k)}$ m-tuple is a set of m elements such that the product of any k of them, increased by 1, is a square.

Our triples $\{a, b, c\}$ correspond to $D^{(3)}$ quadruples

$$\{1, a, b, c\}.$$

Takahashi's thesis contains infinitely many rational $D^{(3)}$ quadruples and conjectures that there are infinitely many integer $D^{(3)}$ quadruples.

The next theorem proves this conjecture.

Theorem 1: **(D. & Szalay (2025))** There are infinitely many triples of positive integers $a, b, c > 1$ such that

$$ab + 1, \quad ac + 1, \quad bc + 1, \quad abc + 1$$

are all perfect squares.

The construction is elementary. It is motivated by numerical examples and the properties of regular Diophantine triples.

Proof of Theorem 1:

Assume

$$ab + 1 = r^2,$$

and put

$$c = a + b + 2r.$$

Then

$$ac + 1 = (a + r)^2, \qquad bc + 1 = (b + r)^2.$$

Diophantine triples of this form are called regular.

Thus, for regular triples only one condition remains:

$$abc + 1 \quad \text{is a square.}$$

Many examples contain the element a of the form

$$a = A^2 + 4.$$

$$\begin{array}{rl} (8 = 2^2 + 4, 45, 91), & (8 = 2^2 + 4, 105, 171), \\ (40 = 6^2 + 4, 119, 297), & (40 = 6^2 + 4, 2387, 3045), \\ (85 = 9^2 + 4, 672, 1235), & (85 = 9^2 + 4, 11859, 13952), \\ (533 = 23^2 + 4, 33475, 42456), & (533 = 23^2 + 4, 509736, 543235), \\ (1160 = 34^2 + 4, 165627, 194509), & (1160 = 34^2 + 4, 2449135, 2556897). \end{array}$$

Almost all of these examples follow the following pattern: a is of the form $a = A_n^2 + 4$, where A_n is a (two-sided) binary recursive sequence defined by

$$A_0 = 1, \quad A_1 = 6, \qquad A_{n+1} = 4A_n - A_{n-1}.$$

For $n \geq 1$, the elements of the sequence A_n are: $6, 23, 86, 321, \ldots$, while for $n \leq -1$, the elements of the sequence $-A_{-n}$ are: $2, 9, 34, 127, 474, \ldots$.

Next, we study the values of r (from $ab + 1 = r^2$) in the observed examples. For each a, we had two triples with given property. We will give details for the second (with larger b) triples. We notice that r's have the form

$$r = A_n^2 R_n + A_{n+1} - 2,$$

where

$$R_0 = 2, \quad R_1 = 8, \quad R_n = 4R_{n-1} - R_{n-2} + 1.$$

In the triples with smaller b, we have

$$r = A_n^2 R_{n-1} - A_{n-1} - 2.$$

To simplify manipulations with the above introduced recursive sequences, will we express them in the terms of the sequence

$$P_0 = 0, \quad P_1 = 1, \quad P_n = 4P_{n-1} - P_{n-2}.$$

Let

$$x = P_{n+1}, \qquad y = P_n.$$

Then

$$x^2 - 4xy + y^2 = 1.$$

This Pell-type identity is important ingredient of our construction. It allows to factor the final expression for $abc + 1$ as a square.

With $x = P_{n+1}$ and $y = P_n$, we have

$A_n = x + 2y, \quad A_{n+1} = 6x - y, \quad R_n = (5x - 3y - 1)/2,$

and thus

$$a = 5x^2 - 12xy + 8y^2,$$

$$r = \frac{17}{2}x^3 - \frac{33}{2}x^2y + 14xy^2 - 7y^3 - \frac{5}{2}x^2 + 6xy - 4y^2.$$

Then put

$$b = \frac{r^2 - 1}{a}, \qquad c = a + b + 2r.$$

By construction,

$$ab + 1 = r^2, \quad ac + 1 = (a + r)^2, \quad bc + 1 = (b + r)^2.$$

The remaining identity is the key point:

$$abc + 1 = \frac{1}{4}(22y^5 - 24xy^4 - 8x^2y^3 + 84x^3y^2 - 119x^4y + 58x^5)^2.$$

Here the relation

$$x^2 - 4xy + y^2 = 1$$

is used repeatedly to make the expression homogeneous and then factor it.

This proves Theorem 1.

Example:

For $n = 4$,

$$x = 209, \qquad y = 56.$$

We obtain

$$a = 1435208,$$

$$b = 3841321681771, \qquad c = 3846019113405,$$

and

$$abc + 1 = 4604722693427179^2.$$

Remark: The infinite family above is based on regular Diophantine triples.

A computer search for non-regular triples with the same four-square property found only one example:

$$\{2, 12, 2380\}.$$

This naturally leads to the question whether there are any other non-regular example.

Tomislav Pejković (2025): Are there infinitely many triples of distinct non-zero integers (resp. rationals) (a, b, c) such that

$$a + 1, \quad b + 1, \quad c + 1,$$

$$ab + 1, \quad ac + 1, \quad bc + 1, \quad abc + 1$$

are all squares?

This is Problem 5.17 on the list of *Open problems on Diophantine m-tuples and elliptic curves*, which supplements my recent book.

We call such triples exotic Diophantine triples.

Equivalently, $\{a, b, c\}$ is exotic if

$$\{1, a, b, c\}$$

is a rational Diophantine quadruple and, in addition,

$$abc + 1$$

is a square.

Two examples from the initial search:

$$\left\{8, \frac{312}{529}, \frac{495}{529}\right\},$$

$$\left\{\frac{312}{529}, -\frac{152880}{165649}, -\frac{78374557}{87628321}\right\}.$$

Theorem 2: **(D., Kazalicki & Petričević (2026))**
There exist infinitely many exotic rational Diophantine triples.

Theorem 3: **(D., Kazalicki & Petričević (2026))**
There are no exotic Diophantine triples in positive integers.

Proof of Theorem 2:

To understand the rational examples, we introduce regularity polynomials:

$$r_3(a,b,c) = (a+b-c)^2 - 4(ab+1),$$

$$r_4(a,b,c,d) = (a+b-c-d)^2 - 4(ab+1)(cd+1).$$

A triple is regular if $r_3 = 0$; a quadruple is regular if $r_4 = 0$.

Both r_3 and r_4 are symmetric.

If

$$r_3(1, ab, c) = 0,$$

then

$$ab + 1, \quad c + 1, \quad abc + 1$$

are squares.

If also

$$r_4(1, a, b, c) = 0,$$

then (because of the symmetry) the only missing conditions for $\{a, b, c\}$ to be an exotic Diophantine triple are that

$$a + 1, \qquad b + 1$$

are squares.

Therefore, we put

$$a = r^2 - 1, \qquad b = s^2 - 1,$$

and study the system

$$\begin{aligned} r_3(1, (r^2-1)(s^2-1), c) &= 0, \\ r_4(1, r^2-1, s^2-1, c) &= 0. \end{aligned}$$

The difference factors as

$$(rs-1)(rs+1)(r^2s^2 - 2s^2 - 2r^2 + 5 + 2c) = 0.$$

The factors $rs - 1$ and $rs + 1$ lead to a genus one curve birationally equivalent to

$$E_1 : \quad y^2 = x^3 - 7x - 6.$$

This elliptic curve has Mordell-Weil rank 0 over $\mathbb{Q}$.

So this branch does not give infinitely many solutions.

The remaining branch is

$$c = \frac{-r^2s^2 + 2s^2 + 2r^2 - 5}{2}.$$

Substitution into $r_4 = 0$ leads to genus one curve birationally equivalent to

$$E_2 : \quad y^2 = x^3 - 111x + 450.$$

Here

$$E_2(\mathbb{Q}) = \langle [6, 0],\ [3, -12] \rangle,$$

where $[6, 0]$ has order 2 and $[3, -12]$ has infinite order.

Hence E_2 gives infinitely many rational exotic triples.

For a point $(x, y) \in E_2(\mathbb{Q})$, put

$$u = \frac{2y - 6x + 42}{x^2 - 6x - 3},$$

$$s = \frac{x^2 - 12x + 39 + 2y}{x^2 - 6x - 3},$$

$$r = \frac{(x-3)u^2 + 7u - 1}{3u^2 + 6u - 1},$$

and

$$c = \frac{-r^2s^2 + 2s^2 + 2r^2 - 5}{2}.$$

Then

$$(r^2 - 1, s^2 - 1, c)$$

is exotic, except for finitely many degenerate points.

For example, the points

$$[7,4] = [6,0] - [3,-12],$$

$$[-6,-30] = [6,0] - 2[3,-12]$$

give the initial examples

$$\left\{8, \frac{312}{529}, \frac{495}{529}\right\},$$

$$\left\{\frac{312}{529}, -\frac{152880}{165649}, -\frac{78374557}{87628321}\right\},$$

while the point $[\frac{223}{9}, -\frac{3068}{27}] = [6,0] - 3[3,-12]$ gives

$$\left\{\frac{724255280}{736742449}, -\frac{152880}{165649}, -\frac{63009087694401}{122040649934401}\right\}.$$

This completes the proof of Theorem 2.

Proof of Theorem 3:

Assume that an exotic triple exists in positive integers.

Since $a+1, b+1, c+1$ are squares, we may order

$$3 \le a < b < c.$$

Write

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

$$c+1 = z^2, \quad abc+1 = u^2.$$

Since $\{1, a, b, c\}$ is an integer Diophantine quadruple, a standard lower bound gives

$$c > 4ab.$$

Define the integer

$$M = 2r(zu - st).$$

We have

$$(zu)^2 - (st)^2 = (c+1)(abc+1) - (ac+1)(bc+1)$$

$$= c(a-1)(b-1).$$

Therefore

$$M = \frac{2rc(a-1)(b-1)}{zu+st}.$$

To bound M, we first bound $zu + st$. The lower bound is

$$zu + st > 2c\sqrt{ab}.$$

For the upper bound, from $c > 4ab \geq 12$, we get

$$zu < rc, \qquad st < rc, \qquad zu + st < 2rc.$$

Thus

$$(a-1)(b-1) < M$$

and

$$M < \frac{r}{\sqrt{ab}}(a-1)(b-1).$$

Since

$$\frac{r}{\sqrt{ab}} = \sqrt{1 + \frac{1}{ab}} < 1 + \frac{1}{2ab},$$

we obtain

$$\begin{aligned}(a-1)(b-1) < M &< \left(1 + \frac{1}{2ab}\right)(a-1)(b-1) \\ &< (a-1)(b-1) + 1.\end{aligned}$$

But M is an integer. Contradiction.

So there are no positive integer exotic triples, which proves Theorem 3.

Open problem 1 (non-regular examples):

Are there infinitely many exotic triples (a, b, c) such that

$$\{1, a, b, c\}$$

is not a regular Diophantine quadruple?

In our initial search, we found 56 exotic triples. Among them, 24 have the property that $\{1, a, b, c\}$ is regular quadruple (only two have additional property that $\{1, ab, c\}$ is a regular triple).

Open problem 2 (the five-square integral case):

Suppose that a, b, c are integers such that $1 < a < b < c$ and

$$c + 1, \quad ab + 1, \quad ac + 1, \quad bc + 1, \quad abc + 1$$

are all squares.

Is it true that necessarily $(a, b, c) = (5, 7, 24)$?

The problem is motivated by the proof of Theorem 3. What is special about $(a, b, c) = (5, 7, 24)$? The triples $\{a, b, c\}$ and $\{1, ab, c\}$ are both regular.

Thank you very much
for your attention!