Diophantine *m*-tuples

Zrinka Franušić
Faculty of Sciences, University of Zagreb

UNIC Mathematics Summer School
Istanbul, June, 2025

Table of contents

Why we study Diophantine m-tuples?

Because they ...

- involve mathematical problems that are easy to state but difficult to solve.
- take us from elementary number theory to advanced areas.
- are the combination of accessibility and depth is what makes them so attractive to study.

C.F. Gauss: "*If mathematics is the queen of sciences, then number theory is the queen of mathematics.*"

The set of m (distinct) non-zero integers $\{a_1, a_2, \ldots, a_m\}$ is called a **Diophantine m-tuples** if

$$a_i a_j + 1 = x_{ij}^2 = \square,\ x_{ij} \in \mathbb{Z}$$

for all $1 \leq i < j \leq m$.

Examples:

- **Diophantus** (3rd century): $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$

$$\frac{1}{16}\cdot\frac{33}{16}+1=\left(\frac{17}{16}\right)^2, \frac{1}{16}\cdot\frac{17}{4}+1=\left(\frac{9}{8}\right)^2, \frac{1}{16}\cdot\frac{105}{16}+1=\left(\frac{19}{16}\right)^2,$$

$$\frac{33}{16}\cdot\frac{17}{4}+1=\left(\frac{25}{8}\right)^2, \frac{33}{16}\cdot\frac{105}{16}+1=\left(\frac{61}{16}\right)^2, \frac{17}{4}\cdot\frac{105}{16}+1=\left(\frac{43}{8}\right)^2.$$

- **Fermat** (17th century): $\{1, 3, 8, 120\}$

$$1\cdot3+1=2^2, 1\cdot8+1=3^2, 1\cdot120+1=11^2, 3\cdot8+1=5^2, 3\cdot120+1=19^2, 8\cdot120+1=31^2.$$

- **Remark**: Diophantine m-tuples can be observed in:
  - any commutative ring with unity
  - in the field of rational numbers $\mathbb{Q}$ / *rational Dioph. m-tuples*
- **Problem: How large these sets can be?**
- **Answer**: Depends on the ring!
  Examples:
  $\{1, 3, 8, 120\}$ in $\mathbb{Z}$
  $\{\frac{5}{36}, \frac{5}{4}, \frac{32}{9}, \frac{189}{4}, \frac{665}{1521}, \frac{3213}{676}\}$ in $\mathbb{Q}$
  $\{4, 7+3\sqrt{5}, 7-3\sqrt{5}, 50+22\sqrt{5}, 50-22\sqrt{5}\}$ in $\mathbb{Z}[\sqrt{5}]$

In the ring of integers, the problem is solved.
Here we deal with Diop. m-tuples in $\mathbb{Z}$, i.e. with positive elements (in $\mathbb{N}$).
(The only Diophantine m-tuple/pair with mixed signs is $\{-1, 1\}$.)






On Diophantine pairs

There are infinitely many Diophantine pairs in $\mathbb{N}$!
Example:
$\{1, r^2 - 1\}$ and $\{r - 1, r + 1\}$ are Diophantine pairs ($r > 1$)
(because the product of these two numbers increased by 1 is r^2.)

Moreover, for any $a \in \mathbb{N}$ and

$$b = k^2 a \pm 2k, \;\; k \in \mathbb{N},$$

$\{a, b\}$ is a Diophantine pair. Note that $ab + 1 = (ka \pm 1)^2$.

On Diophantine triples

There are infinitely many Diophantine triples in $\mathbb{N}$!

Example:

$\{k-1, k+1, 4k\}$ a Diophantine triple for any integer $k > 1$.

Indeed,

$(k-1)(k+1)+1 = k^2$, $4k(k-1)+1 = (2k-1)^2$, $4k(k+1)+1 = (2k+1)^2$.

Problem: In how many ways we can extend a given Diophantine pair $\{a, b\}$ to a Diophantine triple $\{a, b, c\}$?

Answer: There are infinitely many c's!

Assume that $\{a, b\}$ is a Diophantine pair and $ab + 1 = r^2$, $r \in \mathbb{N}$.

- I. step: At least one extension of the pair is easy to find!

$\{a, b, c\}$ is a Diophantine triple for

$$c = a + b + 2r \ \text{ or } \ c = a + b - 2r.$$

Let's check!

$$a(a + b \pm 2r) + 1 = a^2 + ab \pm 2ar + 1 = a^2 + r^2 \pm 2ar = (a \pm r)^2.$$

Analogously,

$$b(a + b \pm 2r) + 1 = (b \pm r)^2.$$

(Caution! $a + b + 2r$ is always a good extension, while $a + b - 2r$ can be 0.)

WLOG, $a < b < c$ and $\{a, b, a + b + 2r\}$ is called **regular** Dioph. triple.

- II. step: Let's find some more extensions!

Assume that $a < b$, $ab + 1 = r^2$. We want to find $c > b$ such that

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

for some $s, t > 0$. By eliminating c, we obtain the **Diophantine equation**

$$at^2 - bs^2 = a - b.$$

Multiplying both sides by a, we get

$$(at)^2 - (ab)s^2 = a(a - b). \tag{1}$$

This equation is of the form

$$X^2 - DY^2 = N, \tag{2}$$

where $D > 0$ and $D \neq \square$, and is better known as **Pellian** or **generalized Pell's equation**.

Pell's equation is an equation of the form

$$X^2 - DY^2 = 1. \tag{3}$$

Pell's equation has infinitely many solutions (for $D \in \mathbb{N}$, $D \neq \square$).
Pellian equation (2) might not have solutions, but if it does, it has infinitely many solutions.

Assume that:
- $(X_1, Y_1) \in \mathbb{N}^2$ is a sol. of (2), $X_1^2 - DY_1^2 = N$
- $(U, V) \in \mathbb{N}^2$ is a sol. of (3), $U^2 - DV^2 = 1$
- (X_2, Y_2) given by $X_2 + \sqrt{D}Y_2 = (X_1 + \sqrt{D}Y_1)(U + \sqrt{D}V)$.

(X_2, Y_2) is a solution of (2):

$$\begin{aligned} X_2^2 - DY_2^2 &= (X_2 + \sqrt{D}Y_2)(X_2 - \sqrt{D}Y_2) \\ &= (X_1 + \sqrt{D}Y_1)(U + \sqrt{D}V)(X_1 - \sqrt{D}Y_1)(U - \sqrt{D}V) \\ &= (X_1^2 - DY_1^2)(U^2 - DV^2) \\ &= N \cdot 1 = N \end{aligned}$$

Pell's eq. has infinitely many solutions $\Longrightarrow$
Pellian eq. has infinitely many solutions (if it is solvable).

Is our equation (1)

$$T^2 - (ab)s^2 = a(a-b), T := at$$

solvable in T and s? YES!
This equation has a solution that arises from the regular expansion $c = a + b + 2r$!
Recall that $ac + 1 = (\underbrace{a+r}_{=s})^2$, $bc + 1 = (\underbrace{b+r}_{=t})^2$. So,
$(T_1, s_1) = (a(b + r), a + r)$ is a solution of (1).
If (U, V) is a solution of $X^2 - (ab)Y^2 = 1$, then

$$(a(b + r) + \sqrt{ab}(a + r))(U + \sqrt{ab}V) = T_2 + \sqrt{ab}\, s_2$$

is an another solution of (1).

We have a new extension of Diophantine pair $\{a, b\}$:

$$c_2 := \frac{s_2^2 - 1}{a} = \frac{((a+r)U + a(b+r)V)^2 - 1}{a},$$

if $c_2 \in \mathbb{N}$. Since

$$s_2^2 - 1 \equiv r^2 U^2 - 1 = (ab+1)U^2 - 1 \equiv U^2 - 1 \pmod{a}$$

and

$$U^2 - 1 = abV^2 \equiv 0 \pmod{a},$$

we have $s_2^2 - 1 \equiv 0 \pmod{a}$.
Pell's eq. has infinitely many solutions $\Longrightarrow$
Dioph. pair has infinitely many extensions!

Are these all possible extensions? We cannot say they are!

On Diophantine quadruples

There exist infinitely many Diophantine quadruples!
Examples:

$$\{k, k+2, 4k+4, 4(k+1)(2k+1)(2k+3)\},\ \ k \geq 1$$

$$\{F_{2n}, F_{2n+2}, F_{2n+4}, 4F_{2n+1}F_{2n+2}F_{2n+3}\},\ \ n \geq 0.$$

(Generalizations of Fermat's quadruple $\{1, 3, 8, 120\}$.)
More general, if the sequence (g_n) is defined as:

$$g_0 = 0, g_1 = 1, g_n = pg_{n-1} - g_{n-2},\ \ n \geq 2,$$

where $p \geq 2$ is an integer, then the set

$$\{g_n, g_{n+2}, (p \pm 2)g_{n+1}, 4g_{n+1}((p \pm 2)g_{2n+1} \mp 1)\}$$

had the property of Diophantus.($p = 2, 3$ give the previous sets.)

$$\{P_{2n}, P_{2n+2}, 2P_{2n}, 4Q_{2n}P_{2n+1}Q_{2n+1}\},$$

$$\{P_{2n}, P_{2n+2}, 2P_{2n+2}, 4P_{2n+1}Q_{2n+1}Q_{2n+2}\}$$

What can we say about the extensions of a Diophantine pair or triple to a Diophantine quadruple? It is always possible!

Theorem 1 (Euler,18th century)

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

is a Diophantine quadruple, where $ab+1=r^2$.

Theorem 2 (Arkin, Hogatt and Strauss, 1979)

$$\{a, b, c, a+b+c+2abc+2rst\} \tag{4}$$

is a Diophantine quadruple, where $ab+1=r^2$, $ac+1=s^2$, $bc+1=t^2$.

(4) is called **regular quadruple**

Extending problem: $\{a, b, c\} \to \{a, b, c, d\}$
$\iff$ determining an integer triple (x, y, z) such that

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

By eliminating d, the previous equations reduce to a system of Diophantine equations:

$$ay^2 - bx^2 = a - b, \tag{5}$$
$$az^2 - cx^2 = a - c, \tag{6}$$

i.e. to a system of Pellian equations:

$$(ay)^2 - (ab)x^2 = a(a - b), \tag{7}$$
$$(az)^2 - (ac)x^2 = a(a - c), \tag{8}$$

These systems of the form are not easy to solve!

Solving simultaneous Pellian equations

Application of

Baker's theory on linear forms in logarithms of algebraic numbers

(for specific values of a, b and c).

A *linear form in logarithms of algebraic numbers* is an expression of the form

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n,$$

where $b_1, \ldots, b_n$ are rational numbers and $\alpha_1, \ldots, \alpha_n$ are algebraic numbers.

Baker's result says that Λ cannot be very close to zero and give an explicit lower bound on $|\Lambda|$. So there exists a computable effective constant $C > 0$ such that

$$|\Lambda| > \exp(-C).$$

Connection between Baker's result and the solution to a system of Pellian eq.

The solutions to each Pellian equation in x (common unknow) are approximately equal to

$$\gamma\alpha^m \text{ and } \delta\beta^n, \; m, n \in \mathbb{N}_0,$$

where $\alpha, \beta, \gamma, \delta$ are quadratic irrationalities (i.e. algebraic numbers). Roughly, solving the system is reduced to searching for the numbers m and n such that

$$\gamma\alpha^m \approx \delta\beta^n.$$

By taking logarithm,

$$\underbrace{m \log\alpha - n\log\beta + \log\frac{\gamma}{\delta}}_{\text{linear form in logs of algebraic numbers}} \approx 0.$$

Baker's result gives and an explicit upper bound for m and n,

$$\max\{m, n\} \leq M$$

Problem! The upper bound is often huge (possibly in the range of 10^{30} or more)!
Solution:
Baker-Davenport's reduction based on the expansion into a continued fraction. This looks like an approximation of a real number ϕ by a rational (a convergent of continued fraction of ϕ).

Remark: Another way to obtain an upper bound on the solutions is by using a result on simultaneous approximation of square roots (so-called hypergeometric method from Diophantine approximations). Namely, if we assume that system (5),(6) has some relatively large solution x, y, z, then y/x and z/x represent very good rational approximations (with a common denominator) of the irrational numbers $\sqrt{a/c}$ and $\sqrt{b/c}$.

Can we say something about the extension of a Diohantine triple to a quadruple? It is always possible (by regular extension), but...

Conjecture 1

If $\{a, b, c, d\}$ *is a Diophantine quadruple and* $d > \max\{a, b, c\}$, *then*

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

Conjecture 1 implies that there is no Diophantine quintuple.
Many results support Conjecture 1. Pioneering works:

- Baker and Davenport (1969): Fermat's triple $\{1, 3, 8\}$ can be extended uniquely with $d = 120$ (i.e. to a regular quadruple)
- Dujella (late 1990s): Families of triples of the form $\{k - 1, k + 1, 4k\}$ and $\{F2k, F2k + 2, F2k + 4\}$ extend uniquely.

Our Main Learning Objectives

Goals related to expanding Diophantine pairs to triples, and triples to quadruples:

- Solve Pell's equation using continued fractions.
- Solve Pellian equations.
- Apply Baker's theory on linear forms in logarithms of algebraic numbers.
- Use the Baker–Davenport reduction method, which involves continued fractions.

On Diophatine quintuples

Conjecture 2 (Diophantine quintuple conjecture)

No Diophantine quintuple (in $\mathbb{Z}$) exists!

- Euler added the fifth (rational) element to Fermat's quadruple

$$\{1, 3, 8, 120, \frac{777480}{8288641}\}.$$

- Dujella generalized Euler's construction to an arbitrary Diophantine quadruple $\{a, b, c, d\}$:

$$\frac{(a+b+c+d)(abcd+1)+2abc+2abd+2acd+2bcd \pm 2r_1r_2r_3r_4r_5r_6}{(abcd-1)^2}$$

where
$ab+1=r_1^2,\ ac+1=r_2^2,\ ad+1=r_3^2,\ bc+1=r_4^2,\ bd+1=r_5^2,\ cd+1=r_6^2.$

- In 2004 Dujella made an important breakthrough showing that a Diophantine sextuple does not exist and that there are only finitely many Diophantine quintuples.
- The bound for the number of possible Diophantine quintuples has been improved by several authors

Theorem 3 (He, Togbé and Ziegler, 2019)

There does not exist a Diophantine quintuple in $\mathbb{Z}$.

One of the generalizations of Diophantine sets:

- Replace the unity with an arbitrary element $n \in \mathcal{R}$.

A Diophantine m-tuple with property $D(n)$ or simply $D(n)$-m-tuple in $\mathcal{R}$ is a set $\{a_1, \ldots, a_m\} \subset \mathcal{R} \setminus \{0\}$ such that

$$a_i a_j + n = \square \text{ (is a square of an element of } \mathcal{R}),$$

for $1 \leq i < j \leq m$.

An interesting fact about $D(n)$-quadruples:

- In some rings the existence of $D(n)$-quadruples is related to the representation of n by the binary quadratic form $x^2 - y^2$, i.e.

a $D(n)$-quadruple exists $\Leftrightarrow$ n is a difference of squares

a $D(n)$-quadruple exists $\Leftrightarrow$ n is a difference of squares

Confirmation of this claim:

- $\mathbb{Z}$*
- $\mathbb{Z}[i]$*
- ring of integers of a real quadratic field $\mathbb{Q}(\sqrt{d})$ for a wide class of positive integers d
- ring of integers of imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$* and $\mathbb{Q}(\sqrt{-2})$*
- ring of integers of the pure cubic field $\mathbb{Q}(\sqrt[3]{2})$
- ring of integers of the biquadratic number field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

* - up to finitelly many exceptions, *-partially proved

But (!), in certain rings of the form $\mathbb{Z}[\sqrt{4k+2}]$ there are elements n which are not difference of two squares but there exist a $D(n)$-quadruple. For instance,

$$\{19+6\sqrt{10}, -8+6\sqrt{10}, 35+18\sqrt{10}, 35+42\sqrt{10}\}$$

is a $D(26+6\sqrt{10})$-quadruple and $n = 26+6\sqrt{10}$ cannot be represented as a difference of two squares in $\mathbb{Z}[\sqrt{10}]$

(Chakraborty, Gupta, Hoque, 2023)

Nevertheless, we think it makes sense to investigate the connection between "$D(n)$-quadruples and differences of squares" in some other rings.

a $D(n)$-quadruple exists $\Leftrightarrow$ n is a difference of squares

The verification procedure consists of the following steps:

- Describe the set S of all elements $n \in \mathcal{R}$ that can be represented as a difference of two squares
- Show the non-existence of a $D(n)$-quadruple if $n \notin S$ using congruence types of quadruples
- Construct effectively, via polynomial formulas, a $D(n)$-quadruple for each $n \in S$. For example, $\{m(3k+1)^2+2k, m(3k+2)^2+2k+2, 9m(2k+1)^2+8k+4\}$ has the $D(2m(2k+1)+1)$-property. (Based on the idea that $\{a, b, a+b+2x, a+4b+4x\}$ has a D(n)-property iff $a(a+4b+4x)+n=\square$, where $ab+n=x^2$.)