WHAT IS...

a Diophantine m-tuple?

Andrej Dujella

Communicated by Florian Luca and Cesar E. Silva

A Diophantine m-tuple is a set of m distinct positive integers with the property that the product of any two of its distinct elements plus 1 is a square. If a set of nonzero rationals has the same property, it is called a rational Diophantine m-tuple. Fermat found the first Diophantine quadruple in integers $\{1, 3, 8, 120\}$. Indeed, we have

$$1 \cdot 3 + 1 = 2^2, \quad 1 \cdot 8 + 1 = 3^2, \quad 1 \cdot 120 + 1 = 11^2,$$
$$3 \cdot 8 + 1 = 5^2, \quad 3 \cdot 120 + 1 = 19^2, \quad 8 \cdot 120 + 1 = 31^2.$$

Euler was able to extend Fermat's quadruple to the rational quintuple $\{1, 3, 8, 120, 777480/8288641\}$.

The ancient Greek mathematician Diophantus found the first example of a rational Diophantine quadruple

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

Some of the famous mathematicians of the past, such as Diophantus, Fermat, and Euler, as well as some modern ones such as Fields Medalist Alan Baker, have made important contributions to problems related to Diophantine m-tuples, but many problems still remain open.

It is natural to ask how large sets of Diophantine m-tuples can be. This question is almost completely solved in the integer case. On the other hand, it seems that in the rational case we do not have even a widely accepted conjecture. In particular, no absolute upper bound for the size of rational Diophantine m-tuples is known. The study of this question leads to surprising connections with elliptic curves.

Note that in the definition of (rational) Diophantine m-tuples we excluded the requirement that the product of an element with itself plus 1 is a square. It is obvious that for integers such a condition cannot be satisfied. But for rationals there is no obvious reason why the sets (called strong Diophantine m-tuples) that satisfy these stronger conditions would not exist. For each element a of such a set we have that $a^2 + 1$ is a square; therefore $a = X/Y$, where (X, Y, Z) is a Pythagorean triple, i.e., $X^2 + Y^2 = Z^2$. It is known that there exist infinitely many strong Diophantine triples, while no example of a strong Diophantine quadruple is known.

In the integer case, it is easy to prove that there exist infinitely many integer Diophantine quadruples (there are parametric families for Diophantine quadruples involving polynomials and Fibonacci numbers, such as $\{k, k+2, 4k+4, 16k^3 + 48k^2 + 44k + 12\}$ and $\{F_k, F_{k+2}, F_{k+4}, 4F_{2k+1}F_{2k+2}F_{2k+3}\}$ for $k \geq 1$), while the folklore conjecture is that there does not exist a Diophantine quintuple. The first important result concerning this conjecture was proved in 1969 by Baker and Davenport. Using Baker's theory on linear forms in logarithms of algebraic numbers and a reduction method based on continued fractions, they proved that if d is a positive integer such that $\{1, 3, 8, d\}$ forms a Diophantine quadruple, then d has to be 120. This implies that Fermat's set $\{1, 3, 8, 120\}$ cannot be extended to a Diophantine quintuple. It was proved in 2004 that a Diophantine sextuple does not exist and that there are only finitely many Diophantine quintuples. Since then, the bound on the number of possible Diophantine quintuples has been improved by several authors (at the moment the best bound seems to be $5.441 \cdot 10^{26}$ due to Cipu and Trudgian), but the question of the existence of Diophantine quintuples is still open.

It is known that any Diophantine triple $\{a, b, c\}$ can be extended to a Diophantine quadruple $\{a, b, c, d\}$. Indeed, with $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$, we may take

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

Andrej Dujella is professor at the University of Zagreb and Fellow of the Croatian Academy of Sciences and Arts. His email address is duje@math.hr.

DOI: http://dx.doi.org/10.1090/noti1404

and then $ad+1=(at+rs)^2, bd+1=(bs+rt)^2, cd+1=(cr+st)^2$. Quadruples of this form are called regular, and the stronger version of the Diophantine quintuple conjecture is that all Diophantine quadruples are regular. Fujita proved that any Diophantine quintuple contains a regular Diophantine quadruple.

Here we sketch the ideas used in the proof of finiteness of Diophantine quintuples and other similar results. Extending the Diophantine triple $\{a,b,c\}$, $a<b<c$, to a Diophantine quadruple $\{a,b,c,d\}$ leads to the system $ad+1=x^2$, $bd+1=y^2$, $cd+1=z^2$, and by eliminating d, we get the system of simultaneous Pellian equations:

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

Solutions of Pellian equations are contained in finitely many binary recursive sequences. Thus, the problem leads to finding intersections of binary recursive sequences, i.e., finitely many equations of the form $v_m=w_n$. These sequences satisfy $v_m\approx\alpha\beta^m$, $w_n\approx\gamma\delta^n$ for certain algebraic numbers $\alpha,\beta,\gamma,\delta$ (e.g. in the case of the Diophantine triple $\{1,3,8\}$ treated by Baker and Davenport, $\alpha=(3+\sqrt{3})/3$, $\beta=2+\sqrt{3}$, $\gamma=(4\pm\sqrt{2})/4$, $\delta=3+2\sqrt{2}$), which implies $m\log\beta-n\log\delta+\log\frac{\alpha}{\gamma}\approx 0$. But a consequence of Baker's theory is that a linear combination, with integer coefficients, of logarithms of algebraic numbers which is nonzero cannot be very close to 0. We therefore obtain upper bounds for m,n. To obtain lower bounds, we can use the congruence method, introduced in joint work with Pethő in 1998, and consider $v_m\equiv w_n \pmod{c^2}$. If m,n are small (compared with c), then $\equiv$ can be replaced by $=$, and this (hopefully) leads to a contradiction (if $m,n>2$, i.e., if d does not correspond to a regular quadruple). Therefore, we obtain lower bounds for m,n (small powers of c). Comparing the upper and lower bounds we get a contradiction for large c.

It is likely that we cannot surpass Fermat by constructing Diophantine quintuples. However, in the rational case, there exist larger sets with the same property. Euler found infinitely many rational Diophantine quintuples. The question of the existence of rational Diophantine sextuples remained open for more than two centuries. In 1999 Gibbs found the first rational Diophantine sextuple

$$\left\{\frac{11}{192},\frac{35}{192},\frac{155}{27},\frac{512}{27},\frac{1235}{48},\frac{180873}{16}\right\},$$

while in 2016 Dujella, Kazalicki, Mikić, and Szikszai proved that there exist infinitely many rational Diophantine sextuples. For example, there are infinitely many such sextuples containing the triple $\{15/14,-16/21,7/6\}$, with the simplest example being

$$\left\{\frac{15}{14},-\frac{16}{21},\frac{7}{6},-\frac{1680}{3481},-\frac{910}{1083},\frac{624}{847}\right\}.$$

No example of a rational Diophantine septuple is known. Moreover, we do not know any rational Diophantine quintuple (or even quadruple) that can be extended to two different rational Diophantine sextuples.

We now describe connections between rational Diophantine m-tuples and elliptic curves. Let $\{a,b,c\}$ be a rational Diophantine triple. In order to extend this triple to a quadruple, we have to find a rational x such that $ax+1$, $bx+1$, and $cx+1$ are all squares of rationals. By multiplying these three conditions, we obtain a single condition

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

which is in fact the equation of an elliptic curve (nonsingular cubic curve with a rational point). We will explain below which points on the curve satisfy the original system of equations and give extensions to Diophantine quadruples.

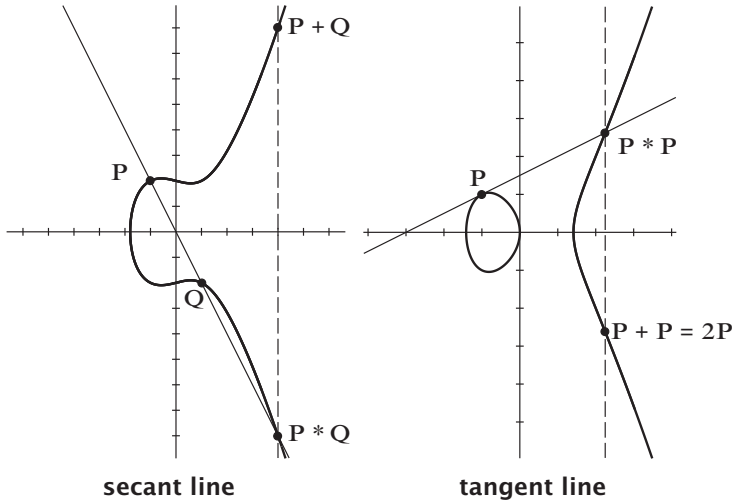


Figure 1. If P and Q have different x-coordinates, then the straight line through P and Q intersects the curve in exactly one more point, denoted by $P*Q$, and we define $P+Q$ as $-(P*Q)$ (where $-(P*Q)$ is the point with the same x-coordinate but negative y-coordinate as $P*Q$). If $P=Q$, then we replace the secant line by the tangent line at the point P.

The set $E(\mathbb{Q})$ of rational points on an elliptic curve E over $\mathbb{Q}$ (affine points $[x,y]$ satisfying the equation along with the point at infinity) forms an abelian group with the law of addition defined by the secant and tangent method as described in the figure.

Moreover, by the Mordell-Weil theorem, the abelian group $E(\mathbb{Q})$ is finitely generated, and hence it is the product of the torsion group and $r\geq 0$ copies of the infinite cyclic group: $E(\mathbb{Q})\cong E(\mathbb{Q})_{\text{tors}}\times\mathbb{Z}^r$.

Let us denote the curve $y^2=(ax+1)(bx+1)(cx+1)$ by $\mathcal{E}$. We say that $\mathcal{E}$ is induced by the Diophantine triple $\{a,b,c\}$. There are three rational points on $\mathcal{E}$ of order 2, namely $A=[-1/a,0]$, $B=[-1/b,0]$, $C=[-1/c,0]$, and also two other obvious rational points:

$$P=[0,1],$$

$$S=[1/abc,\sqrt{(ab+1)(ac+1)(bc+1)}/abc].$$

Note that the x-coordinate of the point $P-S$ is exactly the number d from the definition of regular Diophantine quadruples. In general, P and S will be independent points of infinite order. But an important question, with

significant consequences, is whether they can have finite orders and which orders are possible.

Now we can answer the question which points on $\mathscr{E}$ give extensions to Diophantine quadruples. Namely, the x-coordinate of a point $T \in \mathscr{E}(\mathbb{Q})$ satisfies the original three conditions if and only if $T - P \in 2\mathscr{E}(\mathbb{Q})$. It can be verified that $S \in 2\mathscr{E}(\mathbb{Q})$. This implies that if $x(T)$ satisfies the original conditions, then also the numbers $x(T \pm S)$ satisfy them. It can be shown that $x(T)x(T \pm S) + 1$ is always a perfect square.

Thus, $\{a, b, c, x(T - S), x(T), x(T + S)\}$ is "almost" a rational Diophantine sextuple. The only missing condition is that

$$x(T - S)x(T + S) + 1$$

is a square, and this last condition is satisfied if the point S is of order 3. In that way, the problem of construction of rational Diophantine sextuples becomes closely connected with elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Elliptic curves induced by Diophantine triples were used by Dujella and Peral in 2014 in constructing elliptic curves with given torsion and high rank (details of the current rank records can be found at the webpage `web.math.hr/~duje/tors/tors.html`). It is interesting that any elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ can be induced by a Diophantine triple.

There are several natural generalizations of the notion of Diophantine m-tuples. We can replace squares by k-th powers for fixed $k \geq 3$ (in a joint work with Bugeaud we showed that there are no such quadruples for $k \geq 177$) or by perfect powers (Luca showed in 2005 that the cardinality of such a set is uniformly bounded assuming the abc-conjecture).

We can replace the number 1 in the conditions "$ab + 1$ is a square" by a fixed integer n. Such sets are called $D(n)$-m-tuples. It is easy to show that there are no $D(n)$-quadruples if $n \equiv 2 \pmod 4$. Indeed, assume that $\{a_1, a_2, a_3, a_4\}$ is a $D(n)$-quadruple. Since the square of an integer is $\equiv 0$ or $1 \pmod 4$, we have that $a_i a_j \equiv 2$ or $3 \pmod 4$. This implies that none of the a_i's is divisible by 4. Therefore, we may assume that $a_1 \equiv a_2 \pmod 4$. But now we have that $a_1 a_2 \equiv 0$ or $1 \pmod 4$, a contradiction.

On the other hand, it can be shown that if $n \not\equiv 2 \pmod 4$ and $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there exists at least one $D(n)$-quadruple. For $n \in S$, the question of the existence of $D(n)$-quadruples is still open. No $D(-1)$-quintuple exists, and there are only finitely many such quadruples (and all of them must contain the element 1); among the main contributors here are Filipin and Fuchs. These results solve an old problem investigated by Diophantus and Euler by showing that there does not exist a set of four positive integers with the property that the product of any two of its distinct elements plus their sum is a perfect square. Indeed, since $xy + x + y = (x + 1)(y + 1) - 1$, the existence of such a set would imply the existence of $D(-1)$-quadruples with elements ≥ 2.

Instead of over the integers and rationals, the problem can be considered over any commutative ring with unity. There are interesting results, due to Franušić and Soldo, over rings of integers of certain quadratic fields which show that there is a close connection between existence of a $D(n)$-quadruple and representability of n as a difference of two squares in the ring. Note that integers $\equiv 2 \pmod 4$ are exactly those that cannot be represented as a difference of two squares of integers.

More details on Diophantine m-tuples and the complete list of references can be found at the webpage `web.math.hr/~duje/dtuples.html`.

ABOUT THE AUTHOR

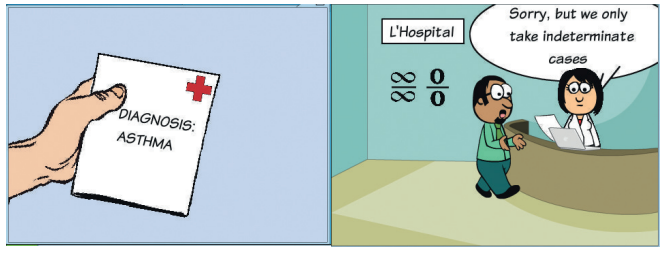
Andrej Dujella received a PhD in mathematics from the University of Zagreb in 1996.

His research interests include Diophantine equations, elliptic curves, polynomial root separation, and applications of Diophantine approximation to cryptography.

Credits

Figure 1 and p. 774 photo, courtesy of Andrej Dujella.

L'Hospital



by Nam Nguyen