$D(n)$-quintuples with square elements

Vinko Petričević
vpetrice@math.hr
http://web.math.hr/~vpetrice/radovi/

PMF-MO Zagreb, Croatia

June 23, 2022

Joint work with Andrej Dujella and Matija Kazalicki

Funding

This work was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Program (Grant KK.01.1.1.01.0004).

Za više informacija posjetite:
http://bela.phy.hr/quantixlie/hr/
https://strukturnifondovi.hr/

For more information:
http://bela.phy.hr/quantixlie/hr/
https://strukturnifondovi.hr/

Sadržaj ove prezentacije isključiva je odgovornost Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu te ne predstavlja nužno stajalište Europske unije.

The content of this presentation is exclusive responsibility of the Faculty of Science University of Zagreb and does not represent opinion of the European Union

EUROPSKA UNIJA
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

Operativni program KONKURENTNOST I KOHEZIJA

Projekt sufinancira Europska unija iz Europskog fonda za regionalni razvoj

Project co-financed by European Union through the European Regional Development Fund

Introduction

For an integer n, a set of m distinct nonzero integers with the property that the product of any two of its distinct elements plus n is a square, is called a Diophantine m-tuple with the property $D(n)$ or $D(n)$-m-tuple. The $D(1)$-m-tuples (with rational elements) are called simply (rational) Diophantine m-tuples, and have been studied since the ancient time.
The first example of a rational Diophantine quadruple was the set

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

found by Diophantus. Fermat found the first Diophantine quadruple in integers $\{1, 3, 8, 120\}$. Euler proved that there exist infinitely many rational Diophantine quintuples), in particular he was able to extend the integer Diophantine quadruple found by Fermat, to the rational quintuple

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

In 2019, Stoll showed that this extension is unique.

In 1969, using linear forms in logarithms of algebraic numbers and a reduction method based on continued fractions, Baker and Davenport 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 result motivated the conjecture that there does not exist a Diophantine quintuple in integers.

The conjecture has been proved 2019. by He, Togbé and Ziegler.

On the other hand, it is not known how large can a rational Diophantine tuple be. In 1999, Gibbs found the first example of rational Diophantine sextuple

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

In 2017, Dujella, Kazalicki, Mikić and Szikszai proved that there are infinitely many rational Diophantine sextuples, while Dujella and Kazalicki (inspired by the work of Piezas) described another construction of parametric families of rational Diophantine sextuples. In 2019, Dujella, Kazalicki and P. proved that there are infinitely many rational Diophantine sextuples such that denominators of all the elements (in the lowest terms) in the sextuples are perfect squares, and (2021) they proved that there are infinitely many Diophantine sextuples containing two regular quadruples and one regular quintuple.

No example of a rational Diophantine septuple is known, but we have many examples of almost septuples (only one condition is missing).

Sets with $D(n)$ properties have also been extensively studied. It is easy to show that there are no integer $D(n)$-quadruples if $n \equiv 2 \pmod 4$, and it is know that if $n \not\equiv 2 \pmod 4$ and $n \notin \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there is at least one $D(n)$-quadruple.
In 2021, Bonciocat, Cipu and Mignotte proved that there are no $D(-1)$-quadruples (as well as $D(-4)$-quadruples) thus leaving the existence of $D(n)$-quadruples in the remaining six sporadic cases open.

In 2000, Dujella proved that for any rational number q there exist infinitely many rational $D(q)$-quadruples, while in 2002. he showed that there are infinitely many rational $D(-1)$-quintuples.
For infinitely many square-free numbers q there are infinitely many rational $D(q)$-quintuples. Assuming the Parity Conjecture for twists of certain elliptic curves, in 2012, Dujella and Fuchs showed that the density of $q \in \mathbb{Q}$ such that there exist infinitely many rational $D(q)$-quintuples is at least $1/2$. The density bound is 2021. improved to at least $49171/49335 \approx 99.5$ by Dražić.
In 2021, Dražić and Kazalicki described rational $D(n)$-quadruples with fixed product of elements. It is not known if there is a rational Diophantine $D(n)$-quintuple for every n, and no example of rational $D(n)$-sextuple is known if n is not a perfect square (but we have many examples of almost sextuples).

In 2001, A. Kihel and O. Kihel asked if there are Diophantine triples $\{a, b, c\}$ which are $D(n)$-triples for several distinct n's. They conjectured that there are no Diophantine triples which are also $D(n)$-triples for some $n \neq 1$. However, Dujella showed 2002, that $\{8, 21, 55\}$ is a $D(1)$ and $D(4321)$-triple, while $\{1, 8, 120\}$ is a $D(1)$ and $D(721)$-triple, as observed by Zhang and Grossman 2015.

In 2017, Adžaga, Dujella, Kreso and Tadić presented several families of Diophantine triples which have $D(n)$-property for two distinct n's with $n \neq 1$ as well as some Diophantine triples which are $D(n)$-sets for three distinct n's with $n \neq 1$.
In 2018, they found examples of Diophantine triples which have $D(n)$-property for three additional n', as well as the set $\{6, 48, 120\}$, which is $D(n)$ set for $n = 36, 1921, 3076, 25956, 110601$.

In 2020, Dujella and P. proved that there are infinitely many (essentially different) integer quadruples which are simultaneously $D(n_1)$-quadruples and $D(n_2)$-quadruples with $n_1 \neq n_2$, and in the same year that the same thing is true for three distinct n's (since the elements of their quadruples are squares, one of n's is equal to zero).

Main result – quintuples

Theorem 1.1

There are infinitely many nonequivalent quintuples that have $D(n_1)$ property for some $n_1 \in \mathbb{N}$ such that all the elements in the quintuple are perfect squares. In particular, there are infinitely many nonequivalent integer quintuples that are simultaneously $D(n_1)$-quintuples and $D(n_2)$-quintuples with $n_1 \neq n_2$ since then we can take $n_2 = 0$.

Note that if $\{a, b, c, d, e\}$ is a $D(n_1)$-quintuple, and u a nonzero rational, then $\{ua, ub, uc, ud, ue\}$ is a $D(n_1 u^2)$-quintuple and we say that these two quintuples are equivalent. Since every rational Diophantine quintuple is equivalent to some $D(u^2)$-quintuple whenever u is an integer divisible by the common denominator of the elements in the quintuple, we proved that there are infinitely many rational Diophantine quintuples with the property that the product of any two of its elements is a perfect square. Details can be found in:

A. Dujella, M. Kazalicki, V. Petričević, *D(n)-quintuples with square elements*, Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **115** (2021), Article 172, (10pp)

In searching for D-sets with m elements, it is natural to first find some sets with $m-1$ element. So let's see what a D-pair could be.

We are actually searching for $D(1)$ and $D(0)$ rational sets in which all elements have the same denominator, and all numerators are squares or $D \times \square$, where D is squarefree.

So for some $a_1, a_2 \in \mathbb{N}$ to be a pair, for some $b \in \mathbb{N}$, then it has to hold $\frac{Da_1^2}{b} \cdot \frac{Da_2^2}{b} + 1 = c^2$, for some $c \in \mathbb{Q}$. Or in the other words, it has to hold $(Da_1 \cdot a_2)^2 + b^2 = c^2$, for $c \in \mathbb{N}$.

Therefore for a fixed b, we calculated all Pythagorean triangles with one leg b. And then $D \cdot a_1 \cdot a_2$ is the other leg. Well known formulas for Pythagorean triples are

$$b = 2dkl \text{ and } Da_1a_2 = d(k+l)(k-l),$$

for some $k, l, d \in \mathbb{N}$, and opposite. (k, l are coprime and one of them is even.)

So we just had to find all divisors of the other leg.

We have implemented the algorithm in C++. To remember pairs, we constructed a graph where each edge is one pair. The graph can be represented using standard containers (for example `map<long, set<long> > g`; so for $a_1 < a_2$, a_1 and a_2 are connected if set `g[`a_2`]` contains a_1). We actually used container `unordered_map<long, vector<long> >`, which is somewhat faster and takes less memory.

So we just had to find the biggest clique in it. Because such a graph is very sparse, it's not hard to do it. On 6-core computer the first quintuple was shown in about 10 seconds:

$$M = \left\{ \frac{225^2}{480480}, \frac{2548^2}{480480}, \frac{286^2}{480480}, \frac{1408^2}{480480}, \frac{819^2}{480480} \right\}$$

which by clearing denominators gives Diophantine $D(480480^2)$-quintuple with square elements.

For example, there are 10 connected Pythagorean triangles: one with legs 480480 and $225 \cdot 2548$, one with the other leg $225 \cdot 286$ and so on. Triangle with legs $225 \cdot 286$ and 480480 is obtained for $(d, k, l) = (4290, 8, 7)$, while the triangle with legs 480480 and $819 \cdot 1408$ is obtained for $(d, k, l) = (96096, 3, 2)$.

We used the simplest algorithm for finding divisors; try to divide with prime numbers $p \leq P$. To check all prime divisors it would be hard because if for example $b = 2k \cdot l$, divisors of $k + l$ could be big (and it is very small possibility that this number is in other D-pairs).

We constructed divisors using factorization and all combinations of exponents, so for known factorizations of x and y we can easy find all divisors of $x \cdot y$.... Later it turned out that this could work better it some situations if we were using simpler methods.

Using sieve of Eratosthenes we generate all primes $\leq P$. And then check only those primes.

We checked two versions of pairs in algorithm. In one, each numerator is a square, and in the other $D > 1$. The first one is much faster, and the second finds more results.

We first checked only for $P \leq 10^6$. Later we realized that this is too much.

Experimental results from other tests suggested that big D-sets usually have only *small* prime factors; for example, for our first quintuple, $P = 11$ is good enough. For example, let us see for $b \leq N = 480480$ and the first algorithm, on a 6-core computer. For $P = 10^3 \ldots 10^9$ there is no big difference in times, while the last one used a little bit more of memory. So let us see differences between $P = 11$ and $P = 10^3$ (B_m represents number of found sets including maybe some the same, and the last two columns (G_4 and G_5) are number of different sets):

P	B_2	B_3	B_4	B_5	G_4	G_5	time
11	1957115	36897	1948	2	1471	1	13sec
10^3	3629788	51068	2256	5	1618	1	28sec,

while for $P = 99$, algorithm is only one second faster than $P = 10^9$ and only number of $B_2 = 3629040$ is somewhat smaller, and all other is the same.

In the second table we show for $P = 11$ how numbers are changing when we double N, or double it once more:

N	B_2	B_3	B_4	B_5	G_4	G_5	time
$2\times$	3848686	65022	3279	3	2521	1	28sec
$4\times$	7370326	112135	5418	5	4240	2	60sec.

The last number $G_2 = 2$ means that we have found equivalent quintuple.

Family of infinitely many $D(0)$-quintuples

We noticed that first few found nonequivalent quintuples have special structure. A Diophantine quadruple $\{a, b, c, d\}$ is called regular if

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

Definition 3.1

We say that rational Diophantine quintuple $\{a, b, c, d, e\}$ is *exotic* if $abcd = 1$, quadruples $\{a, b, d, e\}$ and $\{a, c, d, e\}$ are regular, and if the product of any two of its elements is a perfect square.

On that way we could create many quintuples using parametrizations on some surfaces, and in the previously mentioned paper we proved that there are infinitely many of them.

Very nice proof can be found in this presentation:
`https://web.math.pmf.unizg.hr/~duje/pdf/hannover2021.pdf`

Open question – are there infinitely many regular quintuples?

After about a week of brute-force searching (on 24-core computer), the fourth found quintuple had not this structure:

$$\left\{\frac{12384^2}{1337776440}, \frac{18130^2}{1337776440}, \frac{30745^2}{1337776440}, \frac{110880^2}{1337776440}, \frac{259259^2}{1337776440}\right\}.$$

A Diophantine quintuple $\{a, b, c, d, e\}$ is called regular if

$$(abcde + 2abc + a + b + c - d - e)^2 = 4(ab + 1)(ac + 1)(bc + 1)(de + 1).$$

The last quintuple is regular quintuple. Later, using parametrizations on some surfaces we were able to find many such quintuples, but we don't know is there infinitely many of them.
We have also found many examples of quintuples in which we have that product of four elements is 1, and we have only one regular quadruple. For example:

$$\left\{\frac{407}{13328}, \frac{9613568}{40384575}, \frac{3825}{6512}, \frac{8794863}{37553}, \frac{104192}{34425}\right\}.$$

Open question – is there Diophantine quintuple with square elements?

While we have found infinitely many rational Diophantine quintuples with $D(0)$ property, it remains open if there is a rational Diophantine quintuple with square elements.

On the other hand, there are infinitely many rational Diophantine quadruples with square elements, for example the following two parametric family has this property

$$a = \frac{3^2(s-1)^2(s+1)^2v^2}{2^2(2s^3-2s+v^2)^2},$$

$$b = \frac{v^2(-4s^3+4s+v^2)^2}{2^2(s+1)^2(s-1)^2(-s^3+s+v^2)^2},$$

$$c = \frac{(2s^3-2s+v^2)^2}{3^2v^2s^2},$$

$$d = \frac{4^2(-s^3+s+v^2)^2s^2}{v^2(-4s^3+4s+v^2)^2}.$$

In all examples we had using brute-force search for Diophantine sets with square elements, quadruples have an extra property that the product $abcd = 1$. This would suggest that there is no quintuple with square elements.

But when we write similar program for such search, after few hours on 6-core computer, we find some for which the product $abcd \neq 1$ (and thousands for which product is 1), for example:

$$\left\{ \left(\frac{18}{77}\right)^2, \left(\frac{55}{96}\right)^2, \left(\frac{56}{15}\right)^2, \left(\frac{340}{77}\right)^2 \right\}.$$

Thank you for your attention!