On $D(n)$-quadruples in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Zrinka Franušić, University of Zagreb
Joint work with Borka Jadrijević

Representation Theory XVI, Dubrovnik, 26.6.2019.

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/

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

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

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

Definition

$\mathcal{R}$ - a commutative ring with the unit 1, $n \in \mathcal{R}$.
A Diophantine quadruple with the property $D(n)$ - a set of 4 distinct non-zero elements in $\mathcal{R}$ with the property that the product of each 2 distinct elements increased by n is a perfect square in $\mathcal{R}$

$$\{z_1, z_2, z_3, z_4\} \subset \mathcal{R} \setminus \{0\}$$

$$z_i \neq z_j, \ z_i z_j + n = \square, \ 1 \leq i < j \leq 4$$

Shortly, a $D(n)$-quadruple. If $n = 1$, it is a Diophantine quadruple.

Basic examples

- $\{1, 33, 68, 105\}$, a $D(256)$-quadruple in $\mathbb{Z}$ (*Diophantus*)
- $\{1, 3, 8, 120\}$, a $D(1)$-quadruple in $\mathbb{Z}$ (*Fermat*)

Motivation

Theorem 1. (Brown, Gupta & Singh, Mohanty & Ramasamy, 1985, Dujella, 1993)
A $D(n)$-quadruple in $\mathbb{Z}$ exists **iff** $n \not\equiv 2 \pmod 4$, except for $n \in \{-4, -3, -1, 3, 5, 8, 12, 20\}$.

Theorem 2. (Dujella, 1997)
A $D(n)$-quadruple in $\mathbb{Z}[i]$ exists **iff** $Im(n) \equiv 0 \pmod 2$ and $n \not\equiv 2 + 2i \pmod 4$, except for $n \in \{2, -2, 1 + 2i, -1 - 2i, 4i, -4i\}$

Remark. Conditions from Thm.1 and Thm.2 are related to the binary quadratic form $x^2 - y^2$ (a *difference of two squares*).

- $n \in \mathbb{Z}$, $n \not\equiv 2 \pmod 4$ **iff** $n = x^2 - y^2$, $x, y \in \mathbb{Z}$
- $\mathbb{Z}[i]$, $Im(n) \equiv 0 \pmod 2$ and $n \not\equiv 2 + 2i \pmod 4$ **iff** $n = x^2 - y^2$, $x, y \in \mathbb{Z}[i]$.

Conjecture.

A $D(n)$-quadruple in $\mathcal{R}$ exists **iff** n can be represented as a difference of two squares of elements in $\mathcal{R}$, up to f.m.e.

("up to f.m.e." is an abbreviation "up to finitely many exceptions")

Conjecture has been verified for the following rings:

- the ring of integers of a real quadratic field $\mathbb{Q}(\sqrt{d})$ (for a wide class of positive integers d, Dujella, F.),
- the ring of integers of imaginary quadratic fields $\mathbb{Q}(\sqrt{-3})$ (Soldo, F.) and $\mathbb{Q}[\sqrt{-2}]^*$ (Dujella, Soldo),
- the ring of integers of the pure cubic field $\mathbb{Q}(\sqrt[3]{2})$ (Jukić Matić, F.)

*-partially proved

Bicyclic biquadratic number field $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

One integral basis of the field $\mathbb{K}$ is

$$\{1, \sqrt{2}, \sqrt{3}, \frac{\sqrt{2}+\sqrt{6}}{2}\}.$$

So, the ring of integers of $\mathbb{K}$ is given by

$$\mathcal{O}_{\mathbb{K}} = \{\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\frac{\sqrt{2}+\sqrt{6}}{2} \ : \ \alpha, \beta, \gamma, \delta \in \mathbb{Z}\}.$$

Every $w \in \mathbb{K}$ has a unique representation of the form

$$w = \alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\frac{\sqrt{2}+\sqrt{6}}{2},$$

$\alpha, \beta, \gamma, \delta \in \mathbb{Q}$ (or $\in \mathbb{Z}$ iff $w \in \mathcal{O}_{\mathbb{K}}$) which will be shortly written as

$$w = (\alpha, \beta, \gamma, \delta) \in \mathbb{Q}^4 \ (\text{or } \ \in \mathbb{Z}^4).$$

A strategy for verification of Conjecture

Step 1 Describe the set of all elements $n \in \mathcal{O}_{\mathbb{K}}$ that can be represented as a difference of squares of two elements in $\mathcal{O}_{\mathbb{K}}$.

Step 2 Show the non-existence of a $D(n)$-quadruple if n cannot be represented as a difference of two squares in $\mathcal{O}_{\mathbb{K}}$ using congruence types of quadruples modulo 2 and modulo 4.

Step 3 Construct effectively, via polynomial formulas, a $D(n)$-quadruple for each n from the set described in Step 1.

Proposition 1. (A characterization of difference of two squares in $\mathcal{O}_{\mathbb{K}}$) $n = (\alpha, \beta, \gamma, \delta) \in \mathcal{O}_{\mathbb{K}}$ is a difference of squares of two integers in $\mathcal{O}_{\mathbb{K}}$ **iff** at least one of the following possibilities is valid:

(i) $\alpha \equiv 1 \pmod 2$ and $\beta \equiv \delta \equiv 0 \pmod 2$,

(ii) $\gamma \equiv 1 \pmod 2$ and $\beta \equiv \delta \equiv 0 \pmod 2$,

(iii) $\alpha \equiv \beta \equiv \gamma \equiv 0 \pmod 2$, $(\alpha, \beta, \gamma) \mod 4 \neq (2, 2, 2)$ and $\delta \equiv 0 \pmod 4$.

Proof. $\Rightarrow$: By checking all the possibilities of $n_1^2 - n_2^2$, $n_1, n_2 \in \mathcal{O}_{\mathbb{K}}$ modulo 2 or 4.

$\Leftarrow$: By the following identities:

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

$$(-b+d, -a+2c+1, b, a-c)^2 - (-b+d, -a+2c+1, b, a-c-1)^2 = (2a, 2b, 1+2c, 2d),$$

$$(b+d, \frac{1}{2}(a-c+1), d, c)^2 - (b+d, \frac{1}{2}(a-c-1), d, c)^2 = (2a, 2b, 2c, 4d)$$

$$\left(\frac{1+a+b}{2} - d, \frac{1+a+b}{2} - c, \frac{1-b+c}{2}, \frac{-a+c}{2} + d\right)^2 -$$
$$\left(\frac{-1+a+b}{2} - d, \frac{-1+a+b}{2} - c, \frac{-1-b+c}{2}, \frac{-a+c}{2} + d\right)^2 = (2a, 2b, 2c, 4d)$$

$$\left(\frac{-a+2b-3c+d}{2}, \frac{a+2b-c-d}{2}, \frac{-a+c+d}{2}, -b+c+1\right)^2 -$$
$$\left(\frac{-a+2b-3c+d}{2} - 1, \frac{a+2b-c-d}{2}, \frac{-a+c+d}{2}, -b+c\right)^2 = (2a+1, 2b, 1+2c, 2d),$$

$$\left(\frac{-3-3a+4b-3c+5d}{2}, \frac{1+a-2b+c-d}{2}, \frac{-1-a+2b-3c+3d}{2}, 2+a-b+2c-2d\right)^2 -$$
$$\left(\frac{-3-3a+4b-3c+5d}{2}, \frac{1+a-2b+c-d}{2}, \frac{-3-a+2b-3c+3d}{2}, 1+a-b+2c-2d\right)^2$$
$$= (2a+1, 2b, 1+2c, 2d),$$

where $a, b, c, d \in \mathbb{Z}$ with appropriate parities.

Proposition 2.

If $n = (\alpha, \beta, \gamma, \delta) \in \mathcal{O}_{\mathbb{K}}$ is not representable as a difference of squares of two integers (i.e. iff

(i) $\beta \equiv 1 \pmod 2$,

(ii) $\delta \equiv 1 \pmod 2$,

(iii) $(\alpha, \beta, \gamma) \mod 2 = (0, 0, 0)$ and $\delta \mod 4 = 2$,

(iv) $(\alpha, \beta, \gamma, \delta) \mod 4 = (2, 2, 2, 0)$),

then a $D(n)$-quadruple in $\mathcal{O}_{\mathbb{K}}$ does not exist.

Proof. (i) We assume that $\{n_1, n_2, n_3, n_4\} \subset \mathcal{O}_{\mathbb{K}}$ is a $D(n)$-quadruple, i.e. $n_i n_j + n = \square$. This leads to an inconsistent system of congruences:

$$a_j b_i + a_i b_j + b_j c_i + b_i c_j + c_j d_i + c_i d_j \equiv 1 \pmod 2,\ 1 \leq i < j \leq 4,$$

where $n_i = (a_i, b_i, c_i, d_i)$.

(iii) Assume that $n \mod 4 = (0, 0, 0, 2)$. We found all *congruence types modulo* 4 of a $D(n)$-triple $\{n_1, n_2, n_3\} \subset \mathcal{O}_{\mathbb{K}}$. (A triple $\{n_1, n_2, n_3\}$ has a congruence type $[c_1, c_2, c_3]$ modulo 4, $n_i \equiv c_i \pmod 4$, where $c_i \in \mathbb{Z}_4^4$.) There are 2 829 056 possible congruence triple-types modulo 4 in $\mathcal{O}_{\mathbb{K}}$, but in this case we get *only* 3584 congruence types and none of them can be extended to a $D(n)$-quadruple.

Constructing a $D(n)$-quadruple

Lemma 1 (Dujella, 1996)

Let $m, k \in \mathcal{R}$. The set

$$\{m, m(3k+1)^2+2k, m(3k+2)^2+2k+2, 9m(2k+1)^2+8k+4\} \quad (1)$$

has the $D(2m(2k+1)+1)$-property*.

Lemma 2

If $u \in \mathcal{R}$ and $\{n_1, n_2, n_3, n_4\}$ is a $D(n)$-quadruple in $\mathcal{R}$, then $\{n_1u, n_2u, n_3u, n_4u\}$ is a $D(nu^2)$-quadruple in $\mathcal{R}$.

Lemma 1+2 $\Rightarrow$

$$\{mu, (m(3k+1)^2+2k)u, (m(3k+2)^2+2k+2)u, (9m(2k+1)^2+8k+4)u\} \quad (2)$$

has the $D((2m(2k+1)+1)u^2)$-property*.

*The set can contain equal elements or elements equal to zero - "f.m.e."

The background of the formula (1)

If $\{a, b\}$ is a $D(n)$-pair in $\mathcal{R}$, i.e. $ab + n = x^2$ for $x \in \mathcal{R}$, then $\{a, b, a + b + 2x\}$ is a $D(n)$-triple since

$$a(a + b + 2x) + n = (a + x)^2, \ b(a + b + 2x) + n = (b + x)^2.$$

Dujella's idea: If $\{a, b\}$ is a $D(n)$-pair, then

$$\{a, b, a + b + 2x, a + 4b + 4x\}$$

has a $D(n)$-property **iff** $a(a + 4b + 4x) + n = \square$.

Since, $ab + n = x^2$, we have

$$3n = (a + 2x)^2 - y^2 = (a + 2x - y)(a + 2x + y).$$

If

$$a + 2x - y = 3,\ a + 2x + y = n$$

then $2a + 4x - 3 = n$ and $ab + n = x^2$ implies
$a(b + 2) = (x - 1)(x - 3)$. For $x = ak + 1$, we have
$b = ak^2 - 2k - 2$ and

$$n = 2a(2k + 1) + 1.$$

Remark. Let $n = u^2 - v^2$. Then the set $\{v, v, 2u + 2v, 4u + 5v\}$ has a $D(u^2 - v^2)$-property.

Application of formula (2)

We try to represent the given $n \in \mathcal{O}_{\mathbb{K}}$ described in Proposition 1, which one of 55 types modulo 4 ,

$$n = (4K, 4L, 4M, 4N) + f = 4n_1 + f,$$

where $n_1, f \in \mathcal{O}_{\mathbb{K}}$ and $f = (a, b, c, d) \in \mathbb{Z}_4^4$ as

$$(2m(2k+1)+1)u^2 = n,$$

for some $m, u, k \in \mathcal{O}_{\mathbb{K}}$. We have found useful to fix elements m, u and consider k as solution of the previous equation;

$$k = \frac{n - u^2(1+2m)}{4mu^2} = \frac{4n_1 + f - u^2(1+2m)}{4mu^2}.$$

Application of formula (2)

In the light of the theory of norms, if k is a integer then

$$4^4\mathcal{N}(m)\mathcal{N}(u)^2 \mid \mathcal{N}(4n_1 + f - u^2(1+2m)),$$

where $\mathcal{N}(\alpha) = \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)$ is a norm of $\alpha \in \mathbb{K}$. So, a good starting point for choosing parameters $m, u \in \mathcal{O}_{\mathbb{K}}$ are units ($\mathcal{N}(\alpha) = \pm 1$), as well as elements of small norm.

Proposition 3.

Let $f \in \mathbb{Z}_4^4$, $f \mod 2 \in \{(0,0,1,0),(1,0,0,0)\}$. There exist $m, u \in \mathcal{O}_{\mathbb{K}}$, $N(m) = \pm 1$, $N(u) = \pm 1$ such that the equation

$$(2m(2k+1)+1)u^2 = 4(K,L,M,N) + f$$

has a solution $k \in \mathcal{O}_{\mathbb{K}}$ for all $K, L, M, N \in \mathbb{Z}$.

f	m	u	k
$(0,0,1,0)$	$(2,0,-1,0)$	$(0,0,0,1)$	$(-1+K, L, M, N)$
$(0,0,1,2)$	$(1,0,1,-1)$	$(1,0,1,-1)$	$(18-25K-35L+45M+14N, 20-28K-40L+49M+15N,$ $-10+15K+21L-25M-7N, -14+21K+30L-35M-10N)$
$(0,0,3,0)$	$(0,1,1,0)$	$(1,0,1,1)$	$(4-K+6M-3N, -2+K-3L-3M+2N,$ $-1+2K-2L-M-N, -2K+4L+N)$
$(0,0,3,2)$	$(1,1,1,1)$	$(0,0,0,1)$	$(-9+5K+9L-9M-3N, -11+7K+8L-12M-3N,$ $5-3K-5L+5M+2N, 8-5K-6L+9M+2N)$
$(0,2,1,0)$	$(0,1,1,0)$	$(0,0,0,1)$	$(-1-3K-4L+6M+N, -1-3K-5L+5M+2N,$ $2K+2L-3M-N, 1+2K+4L-4M-N)$
$(0,2,1,2)$	$(1,0,1,1)$	$(0,1,0,-1)$	$(-1+K-L+3M-2N, -M+N,$ $-1+K-L+M-N, 2-K+2L-M+2N)$
$(0,2,3,0)$	$(0,1,1,0)$	$(0,1,0,-1)$	$(2+3K-4L+6M-5N, -K+L-M+2N,$ $1+2K-2L+3M-3N, -1-2K+4L-4M+5N)$
$(0,2,3,2)$	$(1,0,1,1)$	$(0,0,0,1)$	$(8-5K+5L+9M-2N, -8+4K-8L-7M+3N,$ $(-5+3K-3L-5M+N, 6-3K+6L+5M-2N)$
$(1,0,0,0)$	$(1,0,0,0)$	$(2,0,1,0)$	$(1+7K-12M, 11L-4N, -1-4K+7M, -8L+3N)$
$(1,0,0,2)$	$(0,0,0,1)$	$(1,0,0,0)$	$(-L+N, -K+2M, L, K-M)$
$(1,0,2,0)$	$(2,0,1,0)$	$(1,0,0,0)$	$(-2+2K-3M, 3L-N, 1-K+2M, -2L+N)$
$(1,0,2,2)$	$(1,1,1,1)$	$(1,1,0,0)$	$(-1-3K+5L-3M+4N,$ $-1+2K-2L-M-N, -K+L-3M+3N, 1+K-2L+5M-4N)$
$(1,2,0,0)$	$(1,0,0,0)$	$(1,-1,0,0)$	$(2+3K+4L+2N, 2+2K+3L-2M, 3M+2N, 4M+3N)$
$(1,2,0,2)$	$(0,0,0,1)$	$(0,1,1,0)$	$(-2-6K-5L+6M+5N, -4-5K-8L+10M+2N,$ $3+2K+5L-6M, 1+5K+4L-5M-4N)$
$(1,2,2,0)$	$(0,1,1,0)$	$(1,0,0,0)$	$(-2L+3M-N, -K-L+M+N, K-N, 2L-2M+N)$
$(1,2,2,2)$	$(1,0,1,1)$	$(1,1,0,0)$	$(6-5K+7L+15M-7N, -8+7K-10L-14M+5N,$ $-5+5K-7L-5M, 7-7K+10L+7M)$
$(2,0,1,0)$	$(1,0,0,0)$	$(0,1,0,-1)$	$(1+2K+3M, L+N, 1+K+2M, 2L+3N)$

etc. (for 32 values of f, $f \mod 2 \in \{(0,0,1,0),(1,0,0,0)\}$)

Application of formula (2)

Other cases are more complicated. If u and m with just a slightly larger norm ($\mathcal{N}(u) = \pm 2$, $\mathcal{N}(m) = \pm 2$) are implemented in a polynomial formula, we obtain more subcases (characterized in terms of some congruent conditions on K, L, M, N). Also, for some cases, the original polynomial formula for n is too restrictive. So, we represent n in the form

$$(m(2k+1)+1)u^2 = n,$$

where $k, m, u \in \mathcal{O}_{\mathbb{K}}$. A related $D(n)$-quadruple,

$$\{\frac{mu}{2}, \frac{mu}{2}(3k+1)^2+2ku, \frac{mu}{2}(3k+2)^2+(2k+2)\,u, 9\frac{mu}{2}(2k+1)^2+(8k+4)\,u\}$$

is in $\mathcal{O}_{\mathbb{K}}$ iff $\frac{mu}{2} \in \mathcal{O}_{\mathbb{K}}$.

If a polynomial formula representing a $D(n)$-quadruple contains at least two equal elements or the zero element, then we obtain an exception. So, we have to solve nine equations

$$z_i(k) = 0, i = 2, 3, 4, \ z_i(k) - z_j(k) = 0, 1 \leq i < j \leq 4$$

($z_1 = const \neq 0$). The only integer solutions are $k = 0, -1$. Hence, the exceptions are the elements of the form $n = (\pm 2m + 1)u^2$ or $n = (\pm m + 1)u^2$, where m, u are related to $f = n \mod 4$ (or 8). There are 200 such exceptions and all of them be successfully resolved using techniques described in the following examples.

The exception $n = (4, 0, 1, 0) = 4 + \sqrt{3}$ (for $m = (2, 0, -1, 0)$, $u = (0, 0, 0, 1)$ and $k = 0$). The p. f. gives *improper* $D(n)$-quadruple

$$\{(1, 1, 1, 1), (1, 1, 1, 1), (6, 4, 4, 4), (13, 9, 9, 9)\}.$$

Example 1. With a slight change of m, $m' = (2, 0, 1, 0)$ ("new" unit) and the same u, we have $(2m'(2k' + 1) + 1)u^2 = (4, 0, 1, 0)$ for $k' = (3, 0, -2, 0)$ and the related $D(n)$-quadruple

$$\{(0, 1, 0, 3), (0, -36, 0, 26), (0, -39, 0, 31), (0, -151, 0, 111)\}.$$

Example 2. If we could find $n' \in \mathcal{O}_{\mathbb{K}}$ and $u \in \mathcal{O}_{\mathbb{K}}$ (an unit, if possible) such that:

- $n'u^2 = n$,
- $\{z_1, z_2, z_3, z_4\}$ is a *proper* $D(n')$-quadruple

then $\{z_1u, z_2u, z_3u, z_4u\}$ would be a $D(n)$-quadruple (Lemma 2). In this particular case, $n' = (68, -36, 17, -24)$, $u = (3, 2, 0, 0)$ and the $D(n)$-quadruple is

$$\{(-2, -3, 2, 3), (-190, -165, -422, 597), (-186, -174, -430, 612), (-750, -675, -1706, 2415)\}.$$

Theorem

Let $n \in \mathcal{O}_{\mathbb{K}}$. A $D(n)$-quadruple in $\mathcal{O}_{\mathbb{K}}$ exists if and only if n can be represented as a difference of two squares of elements from $\mathcal{O}_{\mathbb{K}}$.

The fact that there is *no exception* in Conjecture is related to the number of units in the particular ring, i.e. if the unit group of a ring is infinite (like in rings integers of some real quadratic fields), no exception is expected!
If there are only finitely many units in a ring, like in the ring of rational integers and in ring of integers of imaginary quadratic fields, the exceptions occur and it seems that they cannot be eliminated with standard methods.
(The most *prominent exception*, $n = -1$ in $\mathbb{Z}$. The conjecture says that $D(-1)$-quadruple does not exist in $\mathbb{Z}$.)