Report on $D(-1)$-quadruples

Mihai Cipu

IMAR, Bucharest, ROMANIA

Representation Theory XVI
Dubrovnik, 28$^{\text{th}}$ June 2019
(joint work with N. C. Bonciocat and M. Mignotte)

Outline

Terminology

$D(n)-m$-set $=$ set of m positive integers, the product of any two being a perfect square minus n

Terminology

$D(n)-m$-set $=$ set of m positive integers, the product of any two being a perfect square minus n

n-pair $= D(n) - 2$-set

Terminology

$D(n) - m$-set $=$ set of m positive integers, the product of any two being a perfect square minus n

n-pair $= D(n) - 2$-set

n-triple $= D(n) - 3$-set

Terminology

$D(n) - m$-set = set of m positive integers, the product of any two being a perfect square minus n

n-pair $= D(n) - 2$-set

n-triple $= D(n) - 3$-set

n-quadruple $= D(n) - 4$-set

Terminology

$D(n) - m$-set = set of m positive integers, the product of any two being a perfect square minus n

n-pair $= D(n) - 2$-set

n-triple $= D(n) - 3$-set

n-quadruple $= D(n) - 4$-set

n-quintuple $= D(n) - 5$-set

Terminology

$D(n)-m$-set $=$ set of m positive integers, the product of any two being a perfect square minus n

n-pair $= D(n) - 2$-set

n-triple $= D(n) - 3$-set

n-quadruple $= D(n) - 4$-set

n-quintuple $= D(n) - 5$-set

$n = -1 \Longrightarrow$ pardi, tridi, quadi

Fundamental question

How large a $D(n) - m$-set can be?

Fundamental question

How large a $D(n) - m$-set can be?

Infinite if $n = 0$

Fundamental question

How large a $D(n) - m$-set can be?

Infinite if $n = 0$

From now on $n \neq 0$

Fundamental question

How large a $D(n)-m$-set can be?

Infinite if $n = 0$

From now on $n \neq 0$

Dujella 2004 Any $D(n)-m$-set has

$$\begin{array}{ll} m \leq 31 & \text{if } 1 \leq |n| \leq 400 \\ m < 15.476 \log |n| & \text{if } \quad |n| > 400 \end{array}$$

Better answers

Brown, Gupta-Singh, Mohanty-Ramasamy 1985

There are no $D(4k+2)$-quadruples

Better answers

Brown, Gupta-Singh, Mohanty-Ramasamy 1985
There are no $D(4k+2)$-quadruples

Dujella 2004 There are no $D(1)$-sextuples and only finitely many $D(1)$-quintuples

Better answers

Brown, Gupta-Singh, Mohanty-Ramasamy 1985
There are no $D(4k+2)$-quadruples

Dujella 2004 There are no $D(1)$-sextuples and only finitely many $D(1)$-quintuples

Dujella-Luca 2005 Any $D(n)-m$-set with n prime has $m < 3 \cdot 2^{168}$

Better answers

Brown, Gupta-Singh, Mohanty-Ramasamy 1985
There are no $D(4k+2)$-quadruples

Dujella 2004 There are no $D(1)$-sextuples and only finitely many $D(1)$-quintuples

Dujella-Luca 2005 Any $D(n)-m$-set with n prime has $m < 3 \cdot 2^{168}$

Dujella-Fuchs 2005 There is no $D(-1)$-quadruple whose smallest element is ≥ 2. Hence, there is no $D(-1)$-quintuple

Better answers

Brown, Gupta-Singh, Mohanty-Ramasamy 1985 There are no $D(4k+2)$-quadruples

Dujella 2004 There are no $D(1)$-sextuples and only finitely many $D(1)$-quintuples

Dujella-Luca 2005 Any $D(n)-m$-set with n prime has $m < 3 \cdot 2^{168}$

Dujella-Fuchs 2005 There is no $D(-1)$-quadruple whose smallest element is ≥ 2. Hence, there is no $D(-1)$-quintuple

Dujella-Filipin-Fuchs 2007 There are only finitely many $D(-1)$-quadruples

Very recent results

He-Togbé-Ziegler 2019 There is no $D(1)$-quintuple

Very recent results

He-Togbé-Ziegler 2019 There is no $D(1)$-quintuple

Bliznac Trebješanin-Filipin 2019 There is no $D(4)$-quintuple

A conjecture

Dujella 1993 if $n \notin \mathcal{S} := \{-4, -3, -1, 3, 5, 12, 20\}$ and $n \neq 4k + 2$ then there exists at least one $D(n)$-quadruple

A conjecture

Dujella 1993 if $n \notin \mathcal{S} := \{-4, -3, -1, 3, 5, 12, 20\}$ and $n \neq 4k + 2$ then there exists at least one $D(n)$-quadruple

Conjecture for $n \in \mathcal{S}$ does not exist $D(n)$-quadruples

How to find $D(-1)$-sets

Prolongation: start with a pair, extend it to a triple, then to a quadruple . . .

How to find $D(-1)$-sets

Prolongation: start with a pair, extend it to a triple, then to a quadruple ...

Prolongation to a quadruple requires to solve a system of three generalized Pell equations

How to find $D(-1)$-sets

$D(-1)$-quadruples

Mihai Cipu

Prologue
Terminology
Main problems
Existence
A conjecture
Classical approach to find quadi
Starting point
Alternative approach
Different viewpoint
A particular case
The general case
References

Prolongation: start with a pair, extend it to a triple, then to a quadruple ...

Prolongation to a quadruple requires to solve a system of three generalized Pell equations

Throughout $\{1, b, c, d\}$ will be a quadi with $1 < b < c < d$

How to find $D(-1)$-sets

Prolongation: start with a pair, extend it to a triple, then to a quadruple ...

Prolongation to a quadruple requires to solve a system of three generalized Pell equations

Throughout $\{1, b, c, d\}$ will be a quadi with $1 < b < c < d$

r, s, t are the positive integers defined by $b - 1 = r^2$, $c - 1 = s^2$, $bc - 1 = t^2$

Existence of quadis

$\exists$ $D(-1)$-quadruples $\iff$ the system

$$z^2 - cx^2 = c - 1,\ bz^2 - cy^2 = c - b,\ y^2 - bx^2 = b - 1$$

is solvable in positive integers

Existence of quadis

$\exists$ $D(-1)$-quadruples $\Longleftrightarrow$ the system $z^2 - cx^2 = c - 1,\ bz^2 - cy^2 = c - b,\ y^2 - bx^2 = b - 1$ is solvable in positive integers

$\Longleftrightarrow$ $z = v_m = w_n$, where the integer sequences $(v_p)_{p\geq 0}$, $(w_p)_{p\geq 0}$ are given by explicit formulæ

$$v_p = \frac{s}{2}\left((s+\sqrt{c})^{2p} + (s-\sqrt{c})^{2p}\right),$$

$$w_p = \frac{s\sqrt{b}+\rho r\sqrt{c}}{2\sqrt{b}}(t+\sqrt{bc})^{2p} + \frac{s\sqrt{b}-\rho r\sqrt{c}}{2\sqrt{b}}(t-\sqrt{bc})^{2p}$$

for some fixed $\rho \in \{-1, 1\}$

Existence of quadis

$\exists$ $D(-1)$-quadruples $\iff$ the system
$z^2 - cx^2 = c - 1,\ bz^2 - cy^2 = c - b,\ y^2 - bx^2 = b - 1$
is solvable in positive integers

$\iff$ $z = v_m = w_n$, where the integer sequences $(v_p)_{p\geq 0}$, $(w_p)_{p\geq 0}$ are given by explicit formulæ

$$v_p = \frac{s}{2}\left((s+\sqrt{c})^{2p} + (s-\sqrt{c})^{2p}\right),$$

$$w_p = \frac{s\sqrt{b}+\rho r\sqrt{c}}{2\sqrt{b}}(t+\sqrt{bc})^{2p} + \frac{s\sqrt{b}-\rho r\sqrt{c}}{2\sqrt{b}}(t-\sqrt{bc})^{2p}$$

for some fixed $\rho \in \{-1, 1\}$

Similarly for x, y

Classical approach

Establish inequalities between b, c, m, n by transforming equalities of the form $z = v_m$, $z = w_n$ into congruences

Classical approach

Establish inequalities between b, c, m, n by transforming equalities of the form $z = v_m$, $z = w_n$ into congruences

Associate a linear form in three logarithms to $v_m = w_n$ and use Baker's theory to obtain absolute bounds on c

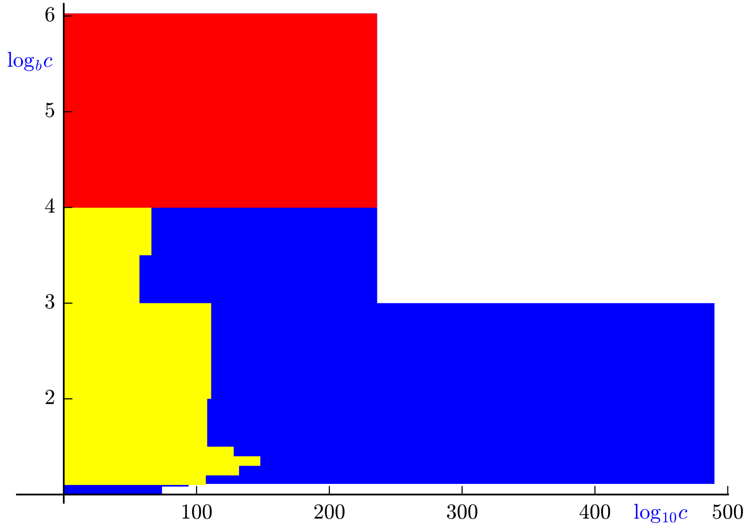
Classical approach

Establish inequalities between b, c, m, n by transforming equalities of the form $z = v_m$, $z = w_n$ into congruences

Associate a linear form in three logarithms to $v_m = w_n$ and use Baker's theory to obtain absolute bounds on c

Long computations give necessary conditions for the existence of $D(-1)$-quadruples, including $b > 1.024 \cdot 10^{13}$ and $\max\{10^{14} b, b^{1.16}\} < c < \min\{9.6\, b^4, 10^{148}\}$

Where to search for quadis



Novel approach

Featuring the positive parameter

$$f = t - rs$$

Novel approach

Featuring the positive parameter

$$f = t - rs$$

Squaring $f + rs = t$, one gets

$$r^2 + s^2 = 2frs + f^2 \qquad (*)$$

Our approach is essentially a study of solutions in positive integers to equation (*) in its various disguises, starting with $(s - rf)^2 - (f^2 - 1)r^2 = f^2$

New results

Theorem

There are no $D(-1)$–quadruples with $f = \gcd(r, s)$. In particular, there exists no $D(-1)$–quadruple for which the corresponding f has no prime divisor congruent to 1 modulo 4.

New results

Theorem

There are no $D(-1)$–quadruples with $f = \gcd(r, s)$. In particular, there exists no $D(-1)$–quadruple for which the corresponding f has no prime divisor congruent to 1 modulo 4.

Theorem

If $c \geq b^2$ then $c > 16b^3$.

Properties in the special case

When $\gcd(r, s) = f$, the cardinal equation has positive solutions

$$r = \frac{f(\gamma^k - \overline{\gamma}^k)}{\gamma - \overline{\gamma}}, \quad s = \frac{f(\gamma^{k+1} - \overline{\gamma}^{k+1})}{\gamma - \overline{\gamma}}, \quad k \in \mathbb{N},$$

with $\gamma = f + \sqrt{f^2 - 1}$ and $\overline{\gamma} = f - \sqrt{f^2 - 1}$

Properties in the special case

When $\gcd(r, s) = f$, the cardinal equation has positive solutions

$$r = \frac{f(\gamma^k - \overline{\gamma}^k)}{\gamma - \overline{\gamma}}, \quad s = \frac{f(\gamma^{k+1} - \overline{\gamma}^{k+1})}{\gamma - \overline{\gamma}}, \quad k \in \mathbb{N},$$

with $\gamma = f + \sqrt{f^2 - 1}$ and $\overline{\gamma} = f - \sqrt{f^2 - 1}$

Always $\quad \gamma^{2k-1} < b \quad$ and $\quad \dfrac{c}{b} < \gamma^2$

Properties in the special case

When $\gcd(r, s) = f$, the cardinal equation has positive solutions

$$r = \frac{f(\gamma^k - \overline{\gamma}^k)}{\gamma - \overline{\gamma}}, \quad s = \frac{f(\gamma^{k+1} - \overline{\gamma}^{k+1})}{\gamma - \overline{\gamma}}, \quad k \in \mathbb{N},$$

with $\gamma = f + \sqrt{f^2 - 1}$ and $\overline{\gamma} = f - \sqrt{f^2 - 1}$

Always $\quad \gamma^{2k-1} < b \quad$ and $\quad \dfrac{c}{b} < \gamma^2$

For $k \geq 2$ it holds $\quad \gamma^2 - \dfrac{1}{2} < \dfrac{c}{b}$

First step in the proof of Theorem A

No quadi has $c > b^3$ in the special case.

First step in the proof of Theorem A

No quadi has $c > b^3$ in the special case.

$$b^3 \le c \Longrightarrow \gamma^{4k-2} < b^2 \le \frac{c}{b} < \gamma^2$$

First step in the proof of Theorem A

No quadi has $c > b^3$ in the special case.

$$b^3 \le c \Longrightarrow \gamma^{4k-2} < b^2 \le \frac{c}{b} < \gamma^2$$

$$\Longrightarrow k < 1$$

First step in the proof of Theorem A

No quadi has $c > b^3$ in the special case.

$$b^3 \le c \Longrightarrow \gamma^{4k-2} < b^2 \le \frac{c}{b} < \gamma^2$$

$$\Longrightarrow k < 1$$

Experimental result: no quadi has $f \le 10^7$. In the special case no quadi has $f \le 10^9$

Second step in the proof of Theorem A

$c \geq b^2 \Longrightarrow k = 1 \Longrightarrow b = f^2 + 1$, $c = 4f^4 + 1$, $t = 2f^3 + f$

Second step in the proof of Theorem A

$$c \geq b^2 \Longrightarrow k = 1 \Longrightarrow b = f^2 + 1,\ c = 4f^4 + 1,$$
$t = 2f^3 + f$

$$v_m \equiv 2f^2 \pmod{8f^6}$$

$$w_n \equiv 2(\rho n + 1)f^2 + \left(\frac{4n^3 + 8n}{3}\rho + 4n^2\right) f^4 \pmod{8f^6}$$

for suitable $\rho \in \{\pm 1\}$

Second step in the proof of Theorem A

$c \geq b^2 \implies k = 1 \implies b = f^2 + 1$, $c = 4f^4 + 1$, $t = 2f^3 + f$

$$v_m \equiv 2f^2 \pmod{8f^6}$$

$$w_n \equiv 2(\rho n + 1)f^2 + \left(\frac{4n^3 + 8n}{3}\rho + 4n^2\right) f^4 \pmod{8f^6}$$

for suitable $\rho \in \{\pm 1\}$

Observe that n is even and use this to deduce $n = 4f^2u$ for some positive integer u. Come back to the congruence to get $u \equiv 0 \pmod{f^2}$, so that $n \geq 4f^4$.

Second step in the proof of Theorem A

$c \geq b^2 \Longrightarrow k = 1 \Longrightarrow b = f^2 + 1$, $c = 4f^4 + 1$, $t = 2f^3 + f$

$$v_m \equiv 2f^2 \pmod{8f^6}$$

$$w_n \equiv 2(\rho n + 1)f^2 + \left(\frac{4n^3 + 8n}{3}\rho + 4n^2\right) f^4 \pmod{8f^6}$$

for suitable $\rho \in \{\pm 1\}$

Observe that n is even and use this to deduce $n = 4f^2 u$ for some positive integer u. Come back to the congruence to get $u \equiv 0 \pmod{f^2}$, so that $n \geq 4f^4$.

This inequality and Matveev's theorem yield $f < 11300$

Third step in the proof of Theorem A

$$b^{3/2} \leq c < b^2 \Longrightarrow k = 2$$

Third step in the proof of Theorem A

$$b^{3/2} \le c < b^2 \Longrightarrow k = 2$$

Now it is preferable to use $y = U_n = u_l$, where

$$u_{l+2} = (4b-2)u_{l+1} - u_l, \qquad u_0 = r, \quad u_1 = (2b-1)r,$$
$$U_{n+2} = (4bc-2)U_{n+1} - U_n, \quad U_0 = \rho r,$$
$$U_1 = (2bc-1)\rho r + 2bst.$$

Third step in the proof of Theorem A

$$b^{3/2} \le c < b^2 \Longrightarrow k = 2$$

Now it is preferable to use $y = U_n = u_l$, where

$$u_{l+2} = (4b-2)u_{l+1} - u_l, \qquad u_0 = r, \quad u_1 = (2b-1)r,$$
$$U_{n+2} = (4bc-2)U_{n+1} - U_n, \quad U_0 = \rho r,$$
$$U_1 = (2bc-1)\rho r + 2bst.$$

The congruence mod r^2 gives $n \ge r - 2 = 2(f^2-1) > 1.999f^2$. From $f > 10^9$ it results $n > 10^{18}$, in contradiction with a previous result

The general case

Write $f = f_1 f_2$, with f_1 the product of all the prime divisors of f which are congruent to 1 modulo 4, multiplicity included. From now on $f_1 \geq 5$

The general case

Write $f = f_1 f_2$, with f_1 the product of all the prime divisors of f which are congruent to 1 modulo 4, multiplicity included. From now on $f_1 \geq 5$

Then $r = f_2 u, \quad s = f_2 v$, with $(v - fu)^2 - (f^2 - 1)u^2 = f_1^2$.

The general case

Write $f = f_1 f_2$, with f_1 the product of all the prime divisors of f which are congruent to 1 modulo 4, multiplicity included. From now on $f_1 \geq 5$

Then $r = f_2 u, \quad s = f_2 v$, with $(v - fu)^2 - (f^2 - 1)u^2 = f_1^2$.

$$r = \frac{f_2\left(\varepsilon\,\gamma^k - \overline{\varepsilon}\,\overline{\gamma}^k\right)}{\gamma - \overline{\gamma}}, \quad s = \frac{f_2\left(\varepsilon\,\gamma^{k+1} - \overline{\varepsilon}\,\overline{\gamma}^{k+1}\right)}{\gamma - \overline{\gamma}}, \quad k \geq 0,$$

with $\varepsilon = v_0 + u_0\sqrt{f^2 - 1}$ a fundamental solution to the generalized Pell equation $V^2 - (f^2 - 1)U^2 = f_1^2$ and $\overline{\varepsilon} = v_0 - u_0\sqrt{f^2 - 1}$.

Properties in the general case

Always $\gamma^{2k} < b$ and $\frac{c}{b} < \gamma^2$

Properties in the general case

Always $\gamma^{2k} < b$ and $\dfrac{c}{b} < \gamma^2$

For $k \geq 1$ it holds $\gamma^2 - \dfrac{1}{2} < \dfrac{c}{b}$

Properties in the general case

Always $\gamma^{2k} < b$ and $\dfrac{c}{b} < \gamma^2$

For $k \geq 1$ it holds $\gamma^2 - \dfrac{1}{2} < \dfrac{c}{b}$

$k = 0 \iff c \geq b^2$

Properties in the general case

Always $\gamma^{2k} < b$ and $\dfrac{c}{b} < \gamma^2$

For $k \geq 1$ it holds $\gamma^2 - \dfrac{1}{2} < \dfrac{c}{b}$

$k = 0 \Longleftrightarrow c \geq b^2$

For $k \geq 1$ it holds

$$f^2 = \left\lceil \frac{c}{4b} \right\rceil .$$

Proof of Theorem B

Theorem

If $c \geq b^2$ *then* $c > 16b^3$.

Proof of Theorem B

Theorem

If $c \geq b^2$ then $c > 16b^3$.

As $k = 0$, one has $r = f_2 u_0$, $s = f_2(v_0 + f u_0)$, with

$$1 \leq v_0 < f_1\sqrt{\frac{f+1}{2}}, \quad 0 \leq |u_0| < \frac{f_1}{\sqrt{2(f+1)}}$$

Proof of Theorem B

Theorem

If $c \geq b^2$ then $c > 16b^3$.

As $k = 0$, one has $r = f_2 u_0$, $s = f_2(v_0 + f u_0)$, with

$$1 \leq v_0 < f_1 \sqrt{\frac{f+1}{2}}, \quad 0 \leq |u_0| < \frac{f_1}{\sqrt{2(f+1)}}$$

$$f_1^2 > 2u_0^2 f = 2u_0^2 f_1 f_2 \implies f_1 > 2u_0^2 f_2 = 2u_0 r$$
$$\implies f = f_1 f_2 > 2u_0 r f_2 = 2r^2$$

Proof of Theorem B

Theorem

If $c \geq b^2$ then $c > 16b^3$.

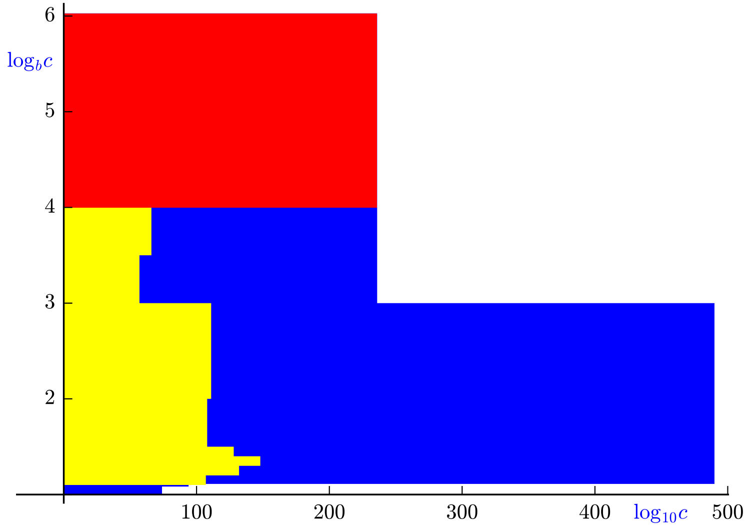
As $k = 0$, one has $r = f_2 u_0$, $s = f_2(v_0 + fu_0)$, with

$$1 \leq v_0 < f_1\sqrt{\frac{f+1}{2}}, \quad 0 \leq |u_0| < \frac{f_1}{\sqrt{2(f+1)}}$$

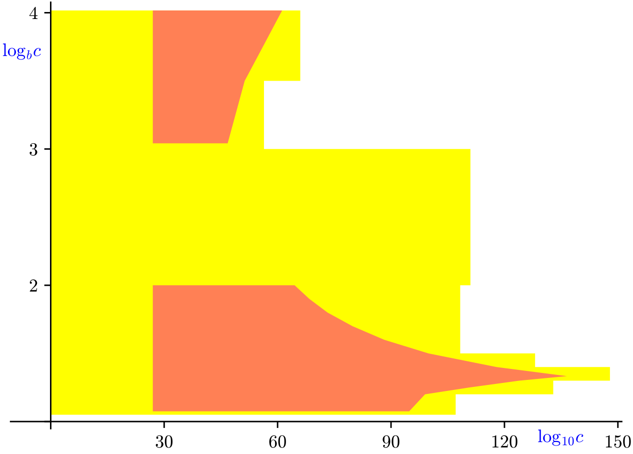
$$f_1^2 > 2u_0^2 f = 2u_0^2 f_1 f_2 \Longrightarrow f_1 > 2u_0^2 f_2 = 2u_0 r$$
$$\Longrightarrow f = f_1 f_2 > 2u_0 r f_2 = 2r^2$$

Put $f = 2r^2 + \delta$ in the cardinal equation to get a quadratic polynomial in s whose discriminant is square only for $\delta = 2r + 1$ or $\geq 4r + 2$

Where we started from



Where are we right now



References 1

A. Baker, H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford Ser. (2)* **20** (1969), 129–137.

M. Bliznac Trebješanin, A. Filipin, Nonexistence of D(4)-quintuples, *J. Number Theory*, **194** (2019), 170-217.

N. C. Bonciocat, M. Cipu, M. Mignotte, On $D(-1)$-quadruples, *Publ. Math.*, **56** (2012), 279–304.

E. Brown, Sets in which $xy + n$ is always a square, *Math. Comp.* **45** (1985), 613–620.

A. Dujella, There are only finitely many Diophantine quintuples, *J. Reine Angew. Math.* **566** (2004), 183–224.

References 2

A. Dujella, Bounds for the size of sets with the property $D(n)$, *Glas. Mat. Ser. III* **39** (2004), 199–205.

A. Dujella, Diophantine m-tuples, http://web.math.pmf.unizg.hr/ duje/dtuples.html

A. Dujella, F. Luca, Diophantine m-tuples for primes, *Intern. Math. Research Notices* **47** (2005), 2913–2940.

A. Dujella, A. Filipin, C. Fuchs, Effective solution of the $D(-1)$-quadruple conjecture, *Acta Arith.* **128** (2007), 319–338.

A. Dujella, C. Fuchs, Complete solution of a problem of Diophantus and Euler, *J. London Math. Soc.* **71** (2005), 33–52.

References 3

A. Filipin, There does not exist a $D(4)$-sextuple, *J. Number Theory* **128** (2008), 1555-1565.

A. Filipin, Y. Fujita, The relative upper bound for the third element of a $D(-1)$–quadruple, *Math. Commun.* **17** (2012), 13–19.

H. Gupta, K. Singh, On k-triad sequences, *Internat. J. Math. Math. Sci.* **5** (1985), 799–804.

B. He, A. Togbé, V. Ziegler, There is no Diophantine quintuple, *Trans. Amer. Math. Soc.* **371** (2019), 6665–6709.

S. P. Mohanty, A. M. S. Ramasamy, On $P_{r,k}$ sequences, *Fibonacci Quart.* **23** (1985), 36–44.