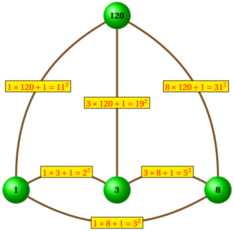
Higher power rational Diophantine tuples

Dubrovnik - Representation Theory XIX

joint work with G. Batta and M. Szikszai

Szabolcs Tengely

24 June 2025



Some known tuples

Where the story (likely) has started:

Diophantus of Alexandria

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

Here we have e.g. $\frac{1}{16} \times \frac{33}{16} + 1 = \left(\frac{17}{16}\right)^2$

Fermat

With integers:

$$\{1, 3, 8, 120\}$$

Some known tuples

Baker and Davenport

$$d \in \mathbb{Z} : \{1, 3, 8, d\} \rightarrow d = 120$$

Euler

$$d \in \mathbb{Q} : \{1, 3, 8, 120, d\} \ \text{example:} \frac{777480}{8288641}$$

Some known tuples

Stoll

$$d \in \mathbb{Q} : \{1, 3, 8, 120, d\} \to d = \frac{777480}{8288641}$$

Euler

An infinite family:

$$ab + 1 = r^2 : \{a, b, a + b + 2r, 4r(r + a)(r + b)\}$$

Higher power tuples

Bugeaud and Dujella

Let $k \geq 3$ and $0 < a < b < c < d$ be integers such that the four numbers

$$ac + 1, ad + 1, bc + 1 \text{ and } bd + 1$$

are perfect k-th powers. Then we have $k \leq 176$.

Examples:
$k = 3 : \{2, 171, 25326\}$
$k = 4 : \{1352, 9539880, 9768370\}$

Higher power tuples

Let $\{a,\ b,\ c\}$ be a quadratic Diophantine triple. A natural idea is the following. Any rational d that extends $\{a,\ b,\ c\}$ into a quadruple is the x-coordinate of some rational point on the elliptic curve

$$E_{a,b,c}:\quad y^2 = (ax+1)(bx+1)(cx+1).$$

Dujella

The x-coordinate of a point $T=(x,y)\in E_{a,b,c}(\mathbb{Q})$ extends the quadratic rational Diophantine triple $\{a,\ b,\ c\}$ into a quadruple if and only if $T-P\in 2E_{a,b,c}(\mathbb{Q})$, where $P=(0,1)$.

Andrej Dujella

Articles with primary MSC 11D ordered according to the number of citations:

MR0718935 - Endlichkeitssätze für abelsche Varietäten über Zahlkörpern
Finiteness theorems for abelian varieties over number fields
Faltings, G.
Invent. Math. **73** (1983), no. 3, 349–366.
(Reviewer: Milne, James)
Reviewed · 650 citations · MSC 11D41 · Article

MR2260521 - The Diophantine Frobenius problem
Ramírez Alfonsín, J. L.
Oxford Lecture Ser. Math. Appl., 30
Oxford University Press, Oxford, 2005, xvi+243 pp.
ISBN: 978-0-19-856820-9; 0-19-856820-7
(Reviewer: Sertöz, Ali Sinan)
Reviewed · Book · 327 citations · MSC 11D72 · Article

MR1863855 - Existence of primitive divisors of Lucas and Lehmer numbers
Bilu, Yu.; Hanrot, G.; Voutier, P. M.
J. Reine Angew. Math. **539** (2001), 75–122.
(Reviewer: Bugeaud, Yann)
Reviewed · 323 citations · MSC 11D59 · Article

MR1645552 - A generalization of a theorem of Baker and Davenport
Dujella, Andrej; Pethő, Attila
Quart. J. Math. Oxford Ser. (2) **49** (1998), no. 195, 291–306.
(Reviewer: Bugeaud, Yann)
Reviewed · 313 citations · MSC 11D09 · Article

MR2215137 - Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers
Bugeaud, Yann; Mignotte, Maurice; Siksek, Samir
Ann. of Math. (2) **163** (2006), no. 3, 969–1018.
(Reviewer: Bilu, Yuri)
Reviewed · 258 citations · MSC 11D61 · Article

MR2076124 - Primary cyclotomic units and a proof of Catalan's conjecture
Mihăilescu, Preda
J. Reine Angew. Math. **572** (2004), 167–195.
(Reviewer: Schoof, René)
Reviewed · 185 citations · MSC 11D61 · Article

MR2039327 - There are only finitely many Diophantine quintuples
Dujella, Andrej
J. Reine Angew. Math. **566** (2004), 183–214.
(Reviewer: Bugeaud, Yann)
Reviewed · 151 citations · MSC 11D09 · Article

MR1923966 - Linear equations in variables which lie in a multiplicative group
Evertse, J.-H.; Schlickewei, H. P.; Schmidt, W. M.
Ann. of Math. (2) **155** (2002), no. 3, 807–836.
(Reviewer: Poulakis, Dimitrios)
Reviewed · 150 citations · MSC 11D04 · Article

MR2031121 - Ternary Diophantine equations via Galois representations and modular forms
Bennett, Michael A.; Skinner, Chris M.
Canad. J. Math. **56** (2004), no. 1, 23–54.
(Reviewer: Darmon, Henri)
Reviewed · 145 citations · MSC 11D41 · Article

MR1348707 - On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$
Darmon, Henri; Granville, Andrew
Bull. London Math. Soc. **27** (1995), no. 6, 513–543.
(Reviewer: Boston, Nigel)
Reviewed · 138 citations · MSC 11D41 · Article

Andrej Dujella

Dujella

There does not exist a Diophantine sextuple.

There are only finitely many Diophantine quintuples.

He, Togbé and Ziegler

There does not exist a Diophantine quintuple.

A Gaussian Generalization

Let $z = a + bi$ be a Gaussian integer. A set of m Gaussian integers is called a complex Diophantine m-tuple with the property $D(z)$ if the product of any two of its distinct elements increased by z is a square of a Gaussian integer.

Dujella

Let l be a Gaussian integer and suppose that the set $\{a, b\} \subset \mathbb{Z}[i]$ has the property $D(l^2)$. If the number ab is not a square of a Gaussian integer, then there exist an infinite number of complex Diophantine quadruples of the form $\{a, b, c, d\}$ with the property $D(l^2)$.

A Gaussian Generalization

An example: $\{1, 2, 5, -24\}$ is a complex Diophantine quadruple with the property $D(-1)$.

$$1 \times 2 - 1 = 1^2, \quad 1 \times 5 - 1 = 2^2, \quad 1 \times (-24) - 1 = (5i)^2$$
$$2 \times 5 - 1 = 3^2, \quad 2 \times (-24) - 1 = (7i)^2, \quad 5 \times (-24) - 1 = (11i)^2.$$

In $\mathbb{Q}(i)$

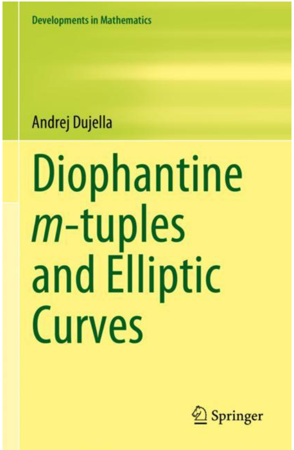
$C: \quad y^2 = -240x^4 + 398x^3 - 175x^2 + 16x + 1 \longrightarrow$

$E: \quad Y^2 = X^3 - 121X^2 + 2000X + 10000$

$\{1, 2, 5, -24, t = \frac{9240}{58081}\}: \quad 1 \times t - 1 = \left(\frac{221i}{241}\right)^2, \quad 2 \times t - 1 = \left(\frac{199i}{241}\right)^2$

$5 \times t - 1 = \left(\frac{109i}{241}\right)^2, \quad (-24) \times t - 1 = \left(\frac{529i}{241}\right)^2.$

Andrej Dujella



Higher power tuples

Gergő Batta used the idea to consider pairs instead of triples together with application of 3-descent in his MSc Thesis. He presented the results at the Number Theory Conference 2022, Debrecen and at the National Student Research Conference (11-13 April 2023, Veszprém), supervisor: Márton Szikszai. He won the first prize. He also presented the results at the 25th Central European Number Theory Conference, 28 August 28 - 1 September, 2023, Sopron, Hungary.
Let $\{a,\ b\}$ be a kth power Diophantine pair and define

$$C_{a,b} : (ay+1)(by+1) = x^k.$$

There are three obvious points:

$$P = (1,0), \qquad A = \left(0, -\frac{1}{a}\right), \qquad B = \left(0, -\frac{1}{b}\right).$$

The case k is odd

The birational change of variables

$$\varphi(x, y) = \left(abx, (ab)^{(k+1)/2} y + \frac{(ab)^{(k-1)/2}(a+b)}{2} \right)$$

transforms $C_{a,b}$ into

$$C'_{a,b} = Y^2 = X^k + \left(\frac{(ab)^{\frac{k-1}{2}}(a-b)}{2} \right)^2 .$$

The coordinates for $P, A,$ and B become

$$P' = \left(ab, \frac{(ab)^{(k-1)/2}(a+b)}{2} \right),$$

$$A' = \left(0, \frac{(ab)^{(k-1)/2}(a-b)}{2} \right), \qquad B' = \left(0, -\frac{(ab)^{(k-1)/2}(a-b)}{2} \right).$$

The case k is even

If k is even we apply

$$\varphi(x,y) = \left(abx, (ab)^{k/2+1}y + \frac{(ab)^{k/2}(a+b)}{2} \right)$$

to get

$$C'_{a,b} = Y^2 = abX^k + \left(\frac{(ab)^{\frac{k}{2}}(a-b)}{2} \right)^2.$$

The rational points P, A, and B change this time into

$$P' = \left(ab, \frac{(ab)^{k/2}(a+b)}{2} \right)$$

$$A' = \left(0, \frac{(ab)^{k/2}(a-b)}{2} \right), \qquad B' = \left(0, -\frac{(ab)^{k/2}(a-b)}{2} \right).$$

Finiteness via Faltings' theorem

Observe that the curve $C_{a,b}$ is a conic for $k = 2$, an elliptic curve if $k = 3$ or 4, and a hyperelliptic curve of genus at least 2 otherwise, in this case by the Faltings' theorem there can be at most finitely many extensions to triples.

Cubic rational Diophantine triples

We have the curve

$$C_{a,b}: \quad (ay+1)(by+1) = x^3$$

or in Weierstrass form:

$$C'_{a,b}: \quad Y^2 = X^3 + \left(\frac{ab(a-b)}{2}\right)^2.$$

the transformations are given by

$$\varphi(x,y) = \left(abx, (ab)^2 y + \frac{ab(a+b)}{2}\right)$$

and

$$\varphi^{-1}(X,Y) = \left(\frac{X}{ab}, \frac{Y - \frac{ab(a+b)}{2}}{(ab)^2}\right).$$

Cubic rational Diophantine triples

The obvious rational points P', A' and B' now have the coordinates

$$\left(ab, \frac{ab(a+b)}{2}\right), \quad \left(0, \frac{ab(a-b)}{2}\right), \quad \left(0, -\frac{ab(a-b)}{2}\right)$$

respectively. Straightforward computation shows the point A', and as a consequence B', has order 3.

3-descent on elliptic curves

Let us follow the description of 3-descent by Cohen and Pazuki. Define $\alpha : C'_{a,b}(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*3}$ as

$$\alpha(R) = \begin{cases} 1 & \text{if } R = \mathcal{O} \\ \frac{1}{ab(a-b)} & \text{if } R = \left(0, \frac{ab(a-b)}{2}\right) \\ Y - \frac{ab(a-b)}{2} & \text{otherwise.} \end{cases}$$

Cohen-Pazuki

The map α is a group homomorphishm.

From 2-descent to 3-descent

Batta-Szikszai-Tengely

Let $\{a, b\}$ be a cubic rational Diophantine pair and $T' \in C'_{a,b}(\mathbb{Q})$. The y-coordinate $y(\varphi^{-1}(T'))$ extends $\{a, b\}$ to a cubic rational Diophantine triple if and only if $P' \neq T'$ is such that $T' - P' \in \ker \alpha$.

Batta-Szikszai-Tengely

Every cubic rational Diophantine pair $\{a,\ b\}$, except $\{-1,\ 1\}$ and $\{-3,\ 3\}$, can be extended into a triple in infinitely many ways. The pairs $\{-1,\ 1\}$ and $\{-3,\ 3\}$ cannot be extended into a triple.

The idea of the proof

First assume that we have a point $T' = (X_0, Y_0) \neq P'$ such that $T' - P' \in \ker \alpha$. We obtain that $\alpha(T') = \alpha(P')$ and the latter one is by definition

$$\alpha(P') = \frac{ab(a+b)}{2} - \frac{ab(a-b)}{2} = ab^2.$$

Therefore there exists a rational $r \neq 0$ such that

$$\alpha(T') = Y_0 - \frac{ab(a-b)}{2} = ab^2 r^3.$$

Let us now compute $\varphi^{-1}(X_0, Y_0) = (x_0, y_0)$, here we only deal with the y-coordinate

$$y_0 = \frac{ab^2 r^3 + \frac{ab(a-b)}{2} - \frac{ab(a+b)}{2}}{a^2 b^2} = \frac{r^3 - 1}{a}.$$

The idea of the proof

One gets that $ay_0 + 1 = r^3$ from the above equation, so it remains to prove that $by_0 + 1$ is also a cube. We know that (x_0, y_0) is a point on $C_{a,b}$ thus we have that

$$(ay_0 + 1)(by_0 + 1) = x_0^3.$$

We also know that $ay_0 + 1 = r^3$. Hence it follows that

$$by_0 + 1 = \left(\frac{x_0}{r}\right)^3.$$

Therefore $\{a, b, y_0\}$ is a cubic Diophantine triple.

The idea of the proof

Consider the other direction, suppose that we have a point (x_0, y_0) on the curve $C_{a,b}$ and $\{a, b, y_0\}$ is a cubic Diophantine triple. We have rational numbers s and t such that $x_0 = st$ and

$$ay_0 + 1 = s^3, \quad by_0 + 1 = t^3.$$

We obtain that $y_0 = \frac{s^3-1}{a}$ and we apply the map φ to compute $\varphi(x_0, y_0)$. The map gives that

$$\varphi(x_0, y_0) = \left(abst, ab^2(s^3 - 1) + \frac{ab(a+b)}{2}\right) = T'.$$

The idea of the proof

Recall that

$$P' = \left(ab, \frac{ab(a+b)}{2} \right).$$

If $P' = T'$, then $st = 1$ and $ab^2(s^3 - 1) = 0$. Since a, b are non-zero rationals we have that $y_0 = 0$, a contradiction. Thus $T' \neq P'$. The image of T' is as follows

$$\alpha(T') = ab^2(s^3 - 1) + \frac{ab(a+b)}{2} - \frac{ab(a-b)}{2} = ab^2 s^3.$$

It follows that $\alpha(P') = \alpha(T')$, therefore $T' - P' \in \ker \alpha$.

Parametric family of triples

Diophantine triples

Let $\{a, b\}$ be a cubic rational Diophantine pair other than $\{-1, 1\}$ and $\{-3, 3\}$. Then $y(-2P)$ extend the pair into a triple, namely

$$\left\{a,\ \ b,\ \ -9\frac{(a^2-ab+b^2)}{(a^3+3a^2b+3ab^2+b^3)}\right\}$$

is a cubic rational Diophantine triple.

Diophantine quadruples

Let $t = r^3, r \in \mathbb{Q}, r \neq 0, \pm 1$. Then

$$\{a, b, c, d\} = \left\{t, -\frac{1}{t}, \frac{-9(t^5+t^3+t)}{(t^6-3t^4+3t^2-1)}, \frac{t^8+5t^6+15t^4+5t^2+1}{(t^7-3t^5+3t^3-t)}\right\}$$

is a cubic rational Diophantine quadruple.

Byeon-Fuchs

Last Friday Clemens Fuchs gave a talk at the Online Seminar of the Number Theory Research Group Debrecen about the same topic. In case of cubic Diophantine tuples they used also 3-descent to prove:

Byeon-Fuchs

Any cube Diophantine pair $\{a, b\}$, except $\{-1, 1\}$ and $\{-3, 3\}$, can be extended to a rational cube Diophantine triple $\{a, b, c\}$.

$\lim_{\text{age} \to 60}$ Dujella

Happy birthday to Professors Dujella, Gusić, and Jadrijević

Thank you for your attention!