STRONG RATIONAL DIOPHANTINE $D(q)$-TRIPLES

ANDREJ DUJELLA, MATTEO PAGANIN, AND MOHAMMAD SADEK

Abstract. We show that for infinitely many square-free integers q there exist infinitely many triples of rational numbers $\{a, b, c\}$ such that $a^2 + q$, $b^2 + q$, $c^2 + q$, $ab + q$, $ac + q$ and $bc + q$ are squares of rational numbers.

1. Introduction

Classically, a *Diophantine m-tuple* is a set $\{a_1, \dots, a_m\}$ of m non-zero integers with the property that $a_i a_j + 1$ is a square, whenever $i \neq j$; such an m-tuple is called *rational* if we allow its elements to be non-zero rational numbers.

Fermat found the first Diophantine quadruple in integers $\{1, 3, 8, 120\}$. In 1969, Baker and Davenport [1] proved that Fermat's set cannot be extended to a Diophantine quintuple. This result motivated the conjecture that there does not exist a Diophantine quintuples in integers. The conjecture has been proved recently by He, Togbé and Ziegler [15].

The first example of a rational Diophantine quadruple, the set $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$ was found by Diophantus, while Euler proved that there exist infinitely many rational Diophantine quintuples (see [16]), In 1999, Gibbs found the first example of rational Diophantine sextuple $\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\}$ (see [13]). In 2017, Dujella, Kazalicki, Mikić and Szikszai [9] proved that there are infinitely many rational Diophantine sextuples, and alternative constructions of families of rational Diophantine sextuples are given in [8], [10] and [11]. It is not known whether there exist any rational Diophantine septuple. More information on Diophantine m-tuples can be found in the survey article [4].

Dujella and Petričević in [12] introduced the notion of *strong* rational Diophantine m-tuple, as a rational Diophantine m-tuple with the additional property that a_i^2+1 is a rational square for every $i = 1, \dots, m$. They proved that there exist infinitely many strong rational Diophantine triples. One such example is the set $\{1976/5607, 3780/1691, 14596/1197\}$.

Let q be a rational number. A set $\{a_1, \dots, a_m\}$ of nonzero integers (rationals) is called a (rational) $D(q)$-m-tuple, if $a_i a_j + q$ is a square of a rational number for all $1 \leq i < j \leq m$. It is known that for every rational number q there exist infinitely many rational $D(q)$-quadruples,

2010 *Mathematics Subject Classification.* 11D09, 11G05.
Key words and phrases. strong Diophantine triples, elliptic curves; twists.

and that there are infinitely many square-free integers q for which there exist infinitely many rational $D(q)$-quintuples (see [3, 5]).

In this paper, we will consider the problem which arises, if we combine the two above mentioned variants of Diophantine m-tuples.

Definition 1.1. Let q be a rational number. A *strong rational Diophantine* $D(q)$*-*m*-tuple* is a set of non-zero rationals $\{a_1, \dots, a_m\}$ such that $a_i a_j + q$ is a square for all $i, j = 1, \dots, m$ (including the case $i = j$).

As we already mentioned, the case $q = 1$ was studied in [12]. The case $q = -1$ was studied in [7] and it was shown that there exist infinitely many strong rational $D(-1)$-triples (in [7] they are called strong Eulerian triples because of the direct connection between $D(-1)$-m-tuples and so called Eulerian m-tuples, which are sets with property that $xy + x + y = (x + 1)(y + 1) - 1$ is a perfect square for all elements x, y of the set).

Our main result is the following theorem.

Theorem 1.2. *There exist infinitely many square-free integers q with the property that there exist infinitely many strong rational Diophantine $D(q)$-triples.*

2. Construction of strong rational Diophantine $D(q)$-pairs and triples

One may see easily that if $\{a_1, \dots, a_m\}$ is a strong rational Diophantine $D(q)$-m-tuple, then $\{za_1, \dots, za_m\}$ is a strong rational Diophantine $D(z^2 q)$-m-tuple. Therefore, it is enough to consider the problem of existence of strong rational Diophantine $D(q)$-triples for square-free integers q, and we will do so in Section 3. Also, since we may choose $z = 1/a_1$ there is no lost of generality if we assume that $a_1 = 1$ and consequently $1^2 + q = r^2$, i.e. $q = r^2 - 1$.

We will now explain a construction of strong rational Diophantine $D(q)$-pairs which uses properties of related elliptic curves.

Proposition 2.1. *For all rational numbers r, $r \neq 0, \pm 1, \pm\frac{1}{2}$, there exist infinitely many rational numbers b such that $\{1, b\}$ is a strong rational Diophantine $D(r^2 - 1)$-pair.*

Proof: For convenience, we set $q = r^2 - 1$. We consider the elliptic curve E^q defined by the equation

$$E^q : \quad y^2 = (x + q)(x^2 + q) = x^3 + qx^2 + qx + q^2.$$

The curve E^q is non-singular for $q \neq 0, -1$, i.e. for $r \neq 0, \pm 1$, so in what follows we will always assume that $r \neq 0, \pm 1$. Some obvious rational points on E^q are

$$T^q = (-q, 0), \qquad P^q = (0, q), \qquad S^q = (1, 1 + q).$$

It is easily checked that $T^q + P^q + S^q = O$.

Any rational number b such that $\{1, b\}$ is a strong rational Diophantine $D(q)$-pair, is the x-coordinate of a point on E^q.

Standard 2-descent (see e.g. [17, 4.2, p.85]) yields that the x-coordinate b of any point in $2E^q(\mathbb{Q})$ satisfies that $\{1, b\}$ is a strong rational Diophantine $D(q)$-pair. Hence, we will finish the proof if we show that E^q has rank at least 1 over $\mathbb{Q}$.

We notice that

$$2S^q = \left(\frac{1}{4} + q, \frac{q}{2} + \frac{1}{8}\right) = \left(\frac{5}{4} - r^2, \frac{r^2}{2} - \frac{3}{8}\right).$$

Assume for the moment that r is an integer. Since the y-coordinate of $2S^q$ cannot be an integer, by the Lutz-Nagell theorem S^q has infinite order and rank(E^q) is at least 1. Let us consider now the general case when r is a rational number. We want to show that again the point S^q has infinite order. By Mazur's classification of torsion points of elliptic curves over $\mathbb{Q}$, it is enough to check that kS^q is not the point at infinity for $k \leq 12$ by considering rational roots of the denominators of the coordinates. We obtain that the only rational roots of denominators are $r = \pm\frac{1}{2}$, in which cases the point S^q is of order 3. For all other rational numbers r, the point S^q is of infinite order. □

By the proof of Proposition 2.1, we may use the x-coordinate of $2kS^{r^2-1}$, k is an integer, to construct families of strong rational Diophantine $D(r^2-1)$-pairs. However, since the x-coordinate of S^{r^2-1} (which is equal to 1) satisfies that conditions that both $x + r^2 - 1$ and $x^2 + r^2 - 1$ are rational squares, by 2-descent, we conclude that we may also use the x-coordinate of $(2k+1)S^{r^2-1}$.

For example, the x-coordinates of $2S^{r^2-1}$, $3S^{r^2-1}$ and $4S^{r^2-1}$ yield that the pairs

$$\left\{1, \frac{5}{4} - r^2\right\}, \qquad \left\{1, \frac{-16r^4 + 16r^2 + 1}{16r^4 - 8r^2 + 1}\right\}, \qquad \left\{1, \frac{256r^8 - 768r^6 + 864r^4 - 496r^2 + 145}{256r^4 - 384r^2 + 144}\right\}$$

are $D(r^2-1)$-pairs.

By extending the first of these three families of pairs, we will construct infinitely many strong rational Diophantine $D(r^2-1)$-triples for rational numbers r of certain form. More precisely, we prove the following proposition.

Proposition 2.2. *For any rational number t different from 0, $\pm\frac{1}{5}$, $\pm\frac{3}{5}$, $\pm\frac{7}{5}$ or $\pm\frac{7}{15}$, the triple*

$$\left\{1, -\frac{625t^4 - 930t^2 + 49}{1024\,t^2}, -\frac{(5t+1)(5t-1)(5t+7)(5t-7)}{1600\,t^2}\right\}$$

is a strong rational Diophantine $D(q)$-triple, with

$$q = \frac{(t-1)(t+1)(25t+7)(25t-7)}{1024\,t^2}.$$

PROOF: In what follows we will use the symbol □ to denote a square of a rational number. A strong rational Diophantine $D(q)$-triple $\{a, b, c\}$ amounts to the following conditions being simultaneously verified:

$$a^2+q=\square_{aa},\quad b^2+q=\square_{bb},\quad c^2+q=\square_{cc},$$
$$ac+q=\square_{ac},\quad ab+q=\square_{ab},\quad bc+q=\square_{bc}.$$

We set $q=r^2-1$, $a=1$, and $b=\dfrac{5}{4}-r^2$, for a rational number $r\neq 0,\pm1,\pm\frac{1}{2}$.

We want to find c, different from 1 and b, such that $\{1,b,c\}$ is a strong Diophantine $D(q)$-triple. From the condition $c+q=s^2$, we shall write $c=s^2-r^2+1$, for some rational number s. We search for such values of the form $s=kr$. The condition $bc+q=\square_{bc}$ then becomes

$$p(k,r)=\frac{5}{4}r^2k^2-r^4k^2-\frac{5}{4}r^2+r^4+\frac{1}{4}=\square_{bc}.$$

This is possible for the values of k that make the discriminant of $p(k,r)$ vanish. The discriminant of $p(k,r)$, with respect to r, is equal to

$$-\frac{1}{64}(5k-3)^2(5k+3)^2(k-1)^3(k+1)^3,$$

so to have $c\neq 1$ we can choose $k=3/5$. Then $p(3/5,r)=\left(\frac{8r^2-5}{10}\right)^2$. Thus, the only condition left is $c^2+q=\square_{cc}$, with $c=-\dfrac{16}{25}r^2+1$, that translates into

$$\frac{1}{625}r^2(256r^2-175)=\square_{cc}.$$

This implies that we need to find $t\in\mathbb{Q}$ such that

$$(256r^2-175)=(16r+25t)^2,$$

that results into the equality $r=-\dfrac{1}{32}\dfrac{25t^2+7}{t}$. Substituting this value in the formulas for b, c, and q, we finally obtain that the triple

$$\left\{1,-\frac{625t^4-930t^2+49}{1024\,t^2},-\frac{(5t+1)(5t-1)(5t+7)(5t-7)}{1600\,t^2}\right\}$$

is a strong rational Diophantine $D\left(\dfrac{(t-1)(t+1)(25t+7)(25t-7)}{1024\,t^2}\right)$-tuple. Finally, the two elements different from 1 are distinct if and only if t is different from $\pm\dfrac{3}{5}$ or $\pm\dfrac{7}{15}$. $\square$

3. Proof of Theorem 1.2

From Proposition 2.2, we only need to prove that, for infinitely many square-free integers q, there are infinitely many rational numbers t such that

$$\frac{(t-1)(t+1)(25t+7)(25t-7)}{1024\,t^2} = qw^2,$$

for some rational number w. Then by dividing all elements of the triple from Proposition 2.2 by w, we get a strong rational $D(q)$-triple.

In other words, we need to study the quartic curve $Q_q : qv^2 = (t-1)(t+1)(25t+7)(25t-7)$. The latter curve is the q-quadratic twist of the curve $Q : v^2 = (t-1)(t+1)(25t+7)(25t-7)$.

The quartic curve Q is birationally equivalent, by the substitutions $t = \frac{144+x}{144-x}$, $v = \frac{576y}{(x-144)^2}$, to the elliptic curve described by the Weierstrass equation:

$$E_1 : y^2 = x(x+81)(x+256);$$

similarly, Q_q is birationally equivalent, by the same substitutions, to

$$E_q : qy^2 = x(x+81)(x+256).$$

We will conclude our proof if we can find infinitely many square-free q for which $\mathrm{rank}(E_q) \geq 1$. We will follow the reasoning from [5]. It is well-known (see e.g. [6]) that for the elliptic curve given by the equation $y^2 = f(x)$, the point $(u, 1)$ is a rational point of infinite order in $E_{f(u)}(\mathbb{Q})$. By writing $u = u_1/u_2$, we get that for all integers q of the form

$$q = u_1u_2(u_1 + 81u_2)(u_1 + 256u_2) \tag{1}$$

the curve E_q has positive rank. This gives us infinitely many square-free values of q for which the rank is positive, and thus for which there exist infinitely many strong rational $D(q)$-quintuples. Indeed, for fixed $\varepsilon > 0$ and sufficiently large N, there are at least $N^{1/2-\varepsilon}$ square-free integers q, $|q| \leq N$, of the form (9) (see e.g. [14]).

□

4. Examples and remarks

We computed the rank of E_q for small values q by `mwrank` [2], and obtained that rank is positive for the following square-free integers in the range $|q| < 100$:

-5, -6, -7, -11, -17, -19, -21, -22, -23, -29, -30, -34, -35, -37, -38, -39, -43, -46, -51, -55,

-57, -58, -61, -62, -66, -67, -69, -74, -77, -78, -79, -83, -85, -86, -87, -91, -93, -94, -95,

2, 6, 10, 13, 15, 17, 23, 26, 29, 30, 31, 33, 35, 37, 42, 46

47, 53, 55, 58, 59, 66, 69, 77, 78, 79, 82, 91, 93, 95.

In next table we give some examples of strong rational $D(q)$-triples $\{a,b,c\}$, for small values of q, obtained by the construction from Theorem 1.2. We provide also the corresponding parameter t.

t	q	a	b	c
$\frac{37}{125}$	-11	$\frac{370}{27}$	$\frac{21122}{4995}$	$\frac{75578}{13875}$
$\frac{11}{25}$	-7	$\frac{44}{9}$	$\frac{1051}{396}$	$\frac{736}{275}$
$\frac{101}{155}$	-6	$\frac{3131}{684}$	$\frac{21031705}{8566416}$	$\frac{591745}{237956}$
$-\frac{23}{25}$	-5	$\frac{23}{3}$	$\frac{709}{276}$	$\frac{1827}{575}$
$-\frac{119}{457}$	2	$\frac{7769}{1638}$	$\frac{38893009}{50902488}$	$\frac{50817649}{35348950}$
$-\frac{23}{265}$	6	$-\frac{1219}{1188}$	$\frac{32386295}{5792688}$	$\frac{542735}{160908}$
$\frac{1}{31}$	10	$\frac{31}{66}$	$-\frac{173279}{8184}$	$-\frac{229437}{17050}$
$\frac{1}{25}$	13	$\frac{2}{3}$	$-\frac{58}{3}$	$-\frac{306}{25}$

Just for fun, we also give a triple for $q=2019$:

$$a = -\frac{1084256489840994627227230285771756902862813585940759 05}{197995600827317846038370910664973564538879492251959 2},$$

$$b = \frac{19903622160350297465727113805280431196879309182571712631429120369343905672609842407986879203598345282474239}{858712060627945518172033052697448822731672169127032763561281839945494931723647684264003999284669990523040},$$

$$c = \frac{2314875761476160622113200620592571545156501721172189311604105086986000693279887159122625184996952958005759}{596327819880517720952800731039895015785883450782661641362001277739927035919199780738891666169909715641000}.$$

Remark 4.1. In Theorem 1.2, the existence of infinitely many square-free integers n for which there are infinitely many $D(n)$-triples mounts down to investigating the Mordell-Weil rank of the quadratic twists $E_q : qy^2 = x(x+81)(x+256)$. Goldfeld's minimalist conjecture asserts that for 50% of square-free integers q, one would expect that $\mathrm{rank}(E_q)$ is positive, hence there are infinitely many strong rational $D(q)$-triples for at least 50% of square-free integers q. See [5] for reasoning how the Parity Conjecture implies that for q's in certain arithmetic progressions the rank of E_q is odd, and hence positive.

Remark 4.2. Note that the elliptic curve E_1, given by the equation $y^2 = x(x+81)(x+256)$ has rank 0 and torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. For curves with such torsion group it is known that there are infinitely many quadratic twists with rank ≥ 4 (see [18, 19]).

Acknowledgements: A. D. acknowledges support from the QuantiXLie Center of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004). A. D. was also supported by the Croatian Science Foundation under the project no. IP-2018-01-1313. This work started while A. D. visited Faculty of Engineering and Natural Sciences, Sabancı University in November 2019. He thanks the colleagues of this institution for their hospitality and support. M. S. was supported by the starting project B.A.CF-19-01964, Sabancı University.

References

[1] A. Baker and 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.

[2] J. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, Cambridge, 1997.

[3] A. Dujella, *A note on Diophantine quintuples*, in: Algebraic Number Theory and Diophantine Analysis (F. Halter-Koch, R. F. Tichy, eds.), Walter de Gruyter, Berlin, 2000, pp. 123–127.

[4] A. Dujella, *What is ... a Diophantine m-tuple?*, Notices Amer. Math. Soc. **63** (2016), 772–774.

[5] A. Dujella and C. Fuchs, *On a problem of Diophantus for rationals*, J. Number Theory **132** (2012), 2075–2083.

[6] A. Dujella, I. Gusić and L. Lasić, *On quadratic twists of elliptic curves* $y^2 = x(x-1)(x-\lambda)$, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **18** (2014), 27–34.

[7] A. Dujella, I. Gusić, V. Petričević and P. Tadić, *Strong Eulerian triples*, Glas. Mat. Ser. III **53** (2018), 33-42.

[8] A. Dujella and M. Kazalicki, *More on Diophantine sextuples*, in: Number Theory - Diophantine problems, uniform distribution and applications, Festschrift in honour of Robert F. Tichy's 60th birthday (C. Elsholtz, P. Grabner, Eds.), Springer-Verlag, Berlin, 2017, pp. 227–235.

[9] A. Dujella, M. Kazalicki, M. Mikić and M. Szikszai, *There are infinitely many rational Diophantine sextuples*, Int. Math. Res. Not. IMRN **2017 (2)** (2017), 490–508.

[10] A. Dujella, M. Kazalicki and V. Petričević, *There are infinitely many rational Diophantine sextuples with square denominators*, J. Number Theory **205** (2019), 340–346.

[11] A. Dujella, M. Kazalicki and V. Petričević, *Rational Diophantine sextuples containing two regular quadruples and one regular quintuple*, Acta Mathematica Spalatensia, to appear.

[12] A. Dujella and V. Petričević, *Strong Diophantine triples*, Experiment. Math. **17** (2008), 83–89.

[13] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), 195–203.

[14] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.

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

[16] T. L. Heath, Diophantus of Alexandria. A Study in the History of Greek Algebra. Powell's Bookstore, Chicago; Martino Publishing, Mansfield Center, 2003.

[17] A. Knapp, Elliptic Curves, Princeton Univ. Press, 1992.
[18] J.-F. Mestre, *Rang de certaines familles de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris **327** (1998), 763–764.
[19] K. Rubin and A. Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Exper. Math. **10** (2001), 559–569.

Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
Email address: duje@math.hr

Foundation Development Program, Sabanci University, Tuzla, İstanbul, 34956 Turkey
Email address: matteo.paganin@sabanciuniv.edu

Faculty of Engineering and Natural Sciences, Sabanci University, Tuzla, İstanbul, 34956 Turkey
Email address: mohammad.sadek@sabanciuniv.edu