On the existence of rational Diophantine quintuples with the property $D(q)$

Andrej Dujella

Department of Mathematics
University of Zagreb, Croatia
e-mail: duje@math.hr
URL: http://web.math.hr/~duje/

Diophantus: Find four numbers such that the product of any two of them, increased by 1, is a perfect square:

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

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

Euler: $\{1, 3, 8, 120, \frac{777480}{8288641}\}$

Gibbs (1999): $\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}$

D. (2009): $\left\{\frac{27}{35}, -\frac{35}{36}, -\frac{352}{315}, \frac{1007}{1260}, -\frac{5600}{4489}, \frac{72765}{106276}\right\}$

Definition: Let q be a nonzero rational number. A set $\{a_1, a_2, \ldots, a_m\}$ of m non-zero integers (rationals) is called *a (rational) Diophantine m-tuple with the property $D(q)$* or *a (rational) $D(q)$-m-tuple* if $a_i \cdot a_j + q$ is a square of a rational number for all $1 \leq i < j \leq m$.

Question: How large such sets can be?

For given q, how large m can be (in integer or in rational case). More precisely, for given q and m, we ask whether there exist any (rational) $D(q)$-m-tuple, and if it exists, whether there exist finitely and infinitely many such m-tuples.

Conjecture: There does not exist a $D(1)$-quintuple.

Baker & Davenport (1969):
$\{1, 3, 8, d\} \Rightarrow d = 120$
(problem raised by Gardner (1967), van Lint (1968))

D. & Pethő (1998):
$\{1, 3\}$ cannot be extended to a $D(1)$-quintuple

Fujita (2008):
$\{k-1, k+1\}$ cannot be extended to a $D(1)$-quintuple

D. (2004): There does not exist a $D(1)$-6-tuple.

There is no known upper bound for the size of rational $D(1)$-tuples.

Some known results in the integer case:

- there are infinitely many $D(n)$-triples for any integer n ($\{a, b, a+b+2r\}$, where $ab+n=r^2$, Diophanus?);

- there exists a $D(256)$-quadruple ($\{1, 33, 68, 105\}$, Diophantus);

- there exists a $D(1)$-quadruple ($\{1, 3, 8, 120\}$, Fermat);

- there are infinitely many $D(1)$-quadruples, and more generally $D(k^2)$-quadruples ($\{a, b, a+b+2r, 4r(a+r)(b+r)\}$, Euler);

- there does not exist a $D(n)$-quadruple for $n \equiv 2 \pmod 4$ (Brown, Gupta & Singh, Mohanty & Ramasamy, 1985);

- if $n \not\equiv 2 \pmod 4$ and $n \notin \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there exist at least one $D(n)$-quadruple (D., 1993);

- there does not exist a $D(1)$-6-tuple (D., 2004), and there are at most finitely many $D(1)$-quintuples (D., 2004);

- there does not exist a $D(4)$-6-tuple (Filipin, 2008), and there are at most finitely many $D(4)$-quintuples (Filipin, 2011);

- there does not exist a $D(-1)$-quintuple (D. & Fuchs, 2005), and there are at most finitely many $D(-1)$-quadruples (D., Filipin & Fuchs, 2007);

- there exist a $D(256)$-quintuple ($\{1, 33, 105, 320, 18240\}$, D., 1997) and a $D(-255)$-quintuple ($\{8, 32, 77, 203, 528\}$, D., 1997);

- there exist a $D(2985984)$-6-tuple ($\{99, 315, 9920, 32768, 44460, 19534284\}$, Gibbs, 1999)

Some known results in the rational case:

- there exists a rational $D(1)$-quadruple ($\{1/16, 33/16, 17/4, 105/16\}$, Diophantus);

- for any rational number q there exist infinitely many rational $D(q)$-quadruples (D., 2000);

- there are infinitely many rational $D(1)$-quintuples (any integer $D(1)$-quadruple of the form $\{a, b, a+b+2r, 4r(a+r)(b+r)\}$ can be extended to a rational $D(1)$-quintuple, e.g. $\{1, 3, 8, 120, 777480/8288641\}$ is a rational $D(1)$-quintuple, Euler),
(any rational $D(1)$-quadruple $\{a, b, c, d\}$ such that $abcd \neq 1$ can be extended to a rational $D(1)$-quintuple, D., 1997);

- a rational $D(1)$-quadruple has at most finitely many extensions to a rational $D(1)$-quintuple (Herrmann, Pethő & Zimmer, 1999);

- there are infinitely many rational $D(-3)$-quintuples (using the fact that the elliptic curve $y^2 = x^3 + 42x^2 + 432x + 1296$ has positive rank, D., 2000);

- there are infinitely many rational $D(-1)$-quintuples (using the fact that the elliptic curve which corresponds to the quartic $y^2 = -(x^2-x-3)(x^2+2x-12)$ has positive rank, D., 2002);

- there exist a rational $D(1)$-sextuple (with positive elements, Gibbs, 1999; for arbitrary choice of signs, D., 2009).

Theorem 1: (D., 2000) *For every rational number q there exist infinitely many distinct rational Diophantine quadruples with the property D(q).*

Proof:
Consider the set

$$\{k, 16k + 8, 25k + 14, 36k + 20\}. \qquad (1)$$

This is a (rational) $D(16k + 9)$-quadruple for all but finitely many integer (rational) k's (an element can be zero, or two elements can be equal). Indeed, the set has the form $\{a, b, a + b + 2r, 4a + b + 4r\}$ and the additional property that $b(4a + b + 4r) + n$ is also a square.

For s a nonzero rational, define the rational number k by $16k + 9 = qs^2$, i.e. $k = \frac{qs^2-9}{16}$. Now from (1) we get a rational $D(q)$-quadruple

$$\left\{\frac{qs^2-9}{16s}, \frac{qs^2-1}{s}, \frac{25qs^2-1}{16s}, \frac{9qs^2-1}{4s}\right\}$$

(for all but finitely many s). We claim that this construction gives infinitely many distinct rational $D(q)$-quadruples. Indeed, only finitely many distinct rationals s can induce the same quadruple, because for $\alpha \in \mathbb{Q}$, the condition $\frac{qs^2-9}{16s} = \alpha$ gives a quadratic equations in s with all most two (rational) solutions, and the same conclusion holds for other elements of the quadruple. $\square$

Question: *For which rational numbers q there exist infinitely many rational $D(q)$-quintuples?*

It is clear that we may restrict our attention to square-free integers q, since by multiplying all elements of a $D(q)$-m-tuple by r we get a $D(qr^2)$-m-tuple.

In the proof of Theorem 1, we have used a polynomial Diophantine quadruple with the property $D(n)$, where n and all element of the quadruple are linear polynomials. There are many other examples of such polynomial quadruples. Thus, we may ask whether there exist any polynomial $D(n)$-quintuple where n and elements of the quintuple are linear polynomials. The answer is: no (D., Fuchs & Walsh (2006), D., Fuchs & Tichy (2002)).

Sketch of the proof: Let $\{ax+b, cx+d, ex+f\}$ be a polynomial $D(ux+v)$-triple, where all coefficients are integers. Then $\{a^2x+ab, acx+ad, aex+af\}$ is a polynomial $D(a^2ux+a^2v)$-triple. By substitution $ax+b=z$ we get a polynomial $D(auz+v')$-triple $\{az, cz+d', ez+f'\}$. We may assume that $\gcd(a,c,e)=1$, since otherwise we substitute $z'=z\gcd(a,c,e)$. This implies that a, c and e are perfect squares:

$$a=A^2, \quad c=C^2, \quad e=E^2,$$

where A, C, E are positive integers. Furthermore, by specializing $z=0$, we see that v' is also a perfect square: $v'=V^2$. But we have

$$v'=a^2v-abu=A^4v-A^2bu=V^2.$$

Hence, $V=AW$ with $W^2=A^2v-bu$.

Now from

$$A^2z \cdot (C^2z + d') + (A^2uz + A^2W^2) = (ACz \pm AW)^2,$$

we find by comparing the coefficients of z that $A^2d' + A^2u = \pm 2A^2CW$ and therefore $d' = \pm 2CW - u$. Analogously, $f' = \pm 2EW - u$. Hence, we obtained the set $\{A^2z, C^2z \pm 2CW - u, E^2z \pm 2EW - u\}$ which is a polynomial $D(A^2uz + A^2W^2)$-triple. It means that

$$(C^2z \pm 2CW - u) \cdot (E^2z \pm 2EW - u) + (A^2uz + A^2W^2)$$

is a square of a linear polynomial and this implies that the discriminant of this quadratic polynomial is equal to 0. The discriminant can be factored into 4 factors:

$$(C-E-A)(C-E+A)(\pm 2CEW - Cu - Eu + Au)(\pm 2CEW - Cu - Eu - Au).$$

The condition $\pm 2CEW - Cu - Eu \pm Au = 0$ can be written as

$$(\pm 2CW - u)(\pm 2EW - u) = u^2 \pm 2AWu.$$

Hence, if there exists a polynomial quintuple with linear polynomails, then there exists a $D(A^2uz + A^2W^2)$-quintuple with one element equal to A^2z, and other elements of the form

$$m_i^2 z + 2m_i W - u, \quad i = 1, 2, 3, 4.$$

Moreover, for $i \neq j$ it holds $|m_i - m_j| = A$ (this corresponds to general construction of triples of the form $\{a, b, a + b \pm 2r\}$) or $(\pm 2m_i W - u)(\pm 2m_j W - u) = u^2 \pm 2AWu$.

D., Fuchs & Walsh (2006) have shown that this these conditions lead to a contradiction. Thus, there does not exist a quintuple with desired property.

However, D. & Fuchs (2012) have shown that these conditions can be fulfilled if we omit just one condition (e.g. $(i, j) = (3, 4)$). Moreover, such "almost quintuple" is essentially unique (all other "almost quintuples" can be obtained from this quintuple by "admissible" transformations). The quintuple is

$$\{x, 9x + 8, 25x + 20, 4x + 2, 16x + 14\}$$

which contains two polynomial $D(10x + 9)$-quadruples:

$$\{x, 9x + 8, 25x + 20, 4x + 2\}$$

and

$$\{x, 9x + 8, 25x + 20, 16x + 14\}.$$

Hence, for a rational number x, the set

$$\{x, 4x+2, 9x+8, 16x+14, 25x+20\}$$

is a rational $D(10x+9)$-quintuple iff

$$(4x+2)(16x+14)+10x+9 = y^2 \qquad (2)$$

for a $y \in \mathbb{Q}$. This is a genus 0 curve. Inserting $y = 8x+t$ in (2), we obtain the parametric solution

$$x = \frac{t^2-37}{2(49-8t)}.$$

Thus, we have proved:

Theorem 2: (D. & Fuchs, 2012) *The set*

$$\{t^2-37, 4t^2-32t+48, 9t^2-128t+451, \\ 16t^2-224t+780, 25t^2-320t+1035\} \qquad (3)$$

is a $D(4(8-t)(5t-32)(8t-49))$*-quintuple.*

Let q be a nonzero rational number. We are interested in the question whether by using Theorem 2 we can get a rational $D(q)$-quintuple. If there exist rationals $s \neq 0$ and t such that

$$4(8-t)(5t-32)(8t-49) = qs^2, \tag{4}$$

then by dividing all elements of (3) by s, we exactly get a $D(q)$-quintuple. The equation (4) defines an elliptic curve over $\mathbb{Q}$. Therefore, we are interested in the question whether these curves have points with nonzero s-coordinate, which leads us to consider curves with positive rank in the family of elliptic curves (for varying q). In fact, this is the family of twists of the elliptic curve given by

$$s^2 = 4(8-t)(5t-32)(8t-49).$$

By the substitutions $t = -x/40 + 49/8, s = y/20$, we get an equation of the curve E in Weierstrass form

$$E\colon\ y^2 = x(x+11)(x+75) = x^3 + 86x^2 + 825x. \quad (5)$$

The curve E has discriminant $D = 2^{16}3^2 5^4 11^2$ and conductor $C = 330 = 2 \cdot 3 \cdot 5 \cdot 11$. Its minimal model is given by $y^2 + xy = x^3 + x^2 - 102x + 324$. Its torsion group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (the only nontrivial torsion points are those with y-coordinate equal 0), and the rank is equal to 1 with the generator $(x, y) = (-15, 60)$.

The question now is which of the q-twists of the curve E have positive rank. As we have already said, we may assume that q is a square-free integer. We consider the family of elliptic curves E_q given by the equation

$$E_q\colon\ qy^2 = x^3 + 86x^2 + 825x. \quad (6)$$

In general, on a curve of the form $f(t)y^2 = f(x)$ there is a rational point $(x, y) = (t, 1)$ of infinite order. If we write $t = u/v$, $\gcd(u, v) = 1$, we get that for q of the form

$$q = uv(u^2 + 86uv + 825v^2), \tag{7}$$

with integers $u, v \neq 0$, there is the point $(u/v, 1/v^2)$ on E_q of infinite order. This gives us infinitely many values of q for which the rank is positive, and thus for which there exist infinitely many rational $D(q)$-quintuples. It can be shown (Gouvêa & Mazur, 1991) that for fixed $\varepsilon > 0$ and sufficiently large N, there are at least $N^{1/2-\varepsilon}$ square-free numbers q, $|q| \leq N$, of the form (7).

Assuming the Parity Conjecture, we can give a precise description of those q's for which the rank of its q-twist is odd (and therefore positive). The Parity Conjecture (for E) says that the rank of the Mordell-Weil group of E is of the same parity as the order of vanishing of the associated L-function $L(E,s)$ at $s=1$. This statement is implied by the Birch and Swinerton-Dyer Conjecture. The Parity Conjeture implies that for an odd square-free integer q relative prime to the conductor C of E, the ranks of E and E_q are equal modulo 2 iff $\chi_q(-C)=1$, where χ_q is the quadratic Dirichlet character associated to $\mathbb{Q}(\sqrt{q})$. Let us mention the Goldfeld Conjecture that says that on taking the average over the ranks of the twists of E we get $1/2$; together with the Parity Conjecture this implies that the number of square-free integers q with $|q| \leq N$ such that E_q has rank 0 (resp. 1) is $6N/\pi^2$ as $N \to \infty$.

Theorem 2: (D. & Fuchs, 2012) *For infinitely many square-free numbers q there are infinitely many rational $D(q)$-quintuples. Assuming the Parity Conjecture for all twists of the elliptic curve E given by* (5) *we get that for all square-free q in at least* 497 *residue classes* (mod 1320) *there are infinitely many rational $D(q)$-quintuples.*

Proof: The first part of the statement has already been almost settled above. It remains to check that at most finitely many distinct points on E_q can induce the same quintuple. For $\alpha \in \mathbb{Q}$, the condition $\frac{t^2-37}{s} = \alpha$ for a point (t, s) on (4) yields a polynomial of degree four in t, so there are at most four points satisfying this condition. The same reasoning applies to other elements of the quintuple.

Let us assume that the Parity Conjecture is true for all twists of E. If $\gcd(q, 330) = 1$, then the Parity Conjecture predicts that the rank of the curve E and the rank of its q-twist have the same parity if and only if $\chi_q(-330) = 1$, where χ_q is the quadratic Dirichlet character attached to the field $\mathbb{Q}(\sqrt{q})$. In particular, if $q \equiv 1 \pmod 4$, then

$$\chi_q(-330) = \left(\frac{-330}{|q|}\right),$$

where $(\frac{\cdot}{\cdot})$ denotes the Jacobi symbol. It follows for all q satisfying

$$\gcd(q, 330) = 1, \ \ q \equiv 1 \pmod 4 \ \text{ and } \ \left(\frac{-330}{|q|}\right) = 1,$$

that the q-twist has odd rank. We find that exactly 80 residue classes (mod $330 \cdot 4 = 1320$) satisfy these conditions.

For $q \equiv 3 \pmod 4$, we consider the q-twist as the $(-q)$-twist of the (-1)-twist of E given by (5). The (-1)-twist has conductor $2^4 \cdot 3 \cdot 5 \cdot 11$ and root number 1 (so that the rank is conjecturally even; but actually one can check that the rank is equal to 0). We therefore get that for all q satisfying

$$\gcd(q, 330) = 1, \ \ q \equiv 3 \pmod 4 \ \text{ and } \ \left(\frac{-165}{|q|}\right) = -1,$$

the rank of the q-twist is odd. This gives us 40 residue classes (mod $165 \cdot 4$), or 80 classes (mod 1320). If $\gcd(q, 330) = g > 1$ we proceed similarly. Let $q = gh$. Then we consider the q-twist as the h-twist of the g-twist of E (or the $(-h)$-twist of the $(-g)$-twist).

For $g \in \{\pm 2, \pm 3, \pm 5, \pm 11, \pm 6, \pm 10, \pm 15, \pm 22, \pm 33, \pm 30, \pm 55, \pm 66, \pm 110, \pm 165, \pm 330\}$ we compute the conductor and the root number of the g-twist. In each case we get that the conductor is of the form $2^k|g|C$ for $k \in \{0, 3, 4\}$. This implies that the conditions we get for q can in all cases be written in terms of residue classes (mod 1320). All together, we get that exactly 497 residue classes (mod 1320) ($q \equiv i \pmod{1320}$, $i = 1, 7, 9, 10, 11, 18, 21, 22, 23, 30, \ldots$) satisfy the condition that the rank of the q-twist is odd. $\square$

It is sufficient for us to find q's such that the twist E_q has rank ≥ 1. We mention that there are indeed curves with rank > 1, e.g. E_{-21} has rank 2, E_{-551} has rank 3, E_{5217} has rank 4, $E_{19712449}$ has rank 5, and $E_{18427939089}$ has rank 6.

Example: The smallest square-free positive integer $q > 1$ for which the above construction gives (infinitely many) $D(q)$-quintuples is $q = 7$. We have the twist $7y^2 = x(x + 11)(x + 75)$ with rank 1 and generator $(x, y) = (-25, 50)$ of the Mordell-Weil group. It induces the point $(t, s) = (27/4, 5/2)$ on (4). From Theorem 2 we obtain the rational $D(7)$-quintuple

$$\left\{\frac{137}{40}, \frac{57}{10}, -\frac{47}{40}, -\frac{6}{5}, \frac{45}{8}\right\}.$$

Let us take now the point $2P = (4/7, 414/49)$. It induces the point $(t, s) = (1711/280, 207/490)$ on (4). From Theorem 2 we obtain the rational $D(7)$-quintuple (with positive elements)

$$\left\{\frac{2969}{3680}, \frac{35681}{8280}, \frac{383849}{33120}, \frac{42401}{2070}, \frac{205285}{6624}\right\}.$$