ON A PROBLEM OF DIOPHANTUS FOR RATIONALS

ANDREJ DUJELLA AND CLEMENS FUCHS

Abstract. Let q be a nonzero rational number. We investigate for which q there are infinitely many sets consisting of five nonzero rational numbers such that the product of any two of them plus q is a square of a rational number. We show that there are infinitely many square-free such q and on assuming the Parity Conjecture for the twists of an explicitly given elliptic curve we derive that the density of such q is at least one half.

For the proof we consider a related question for polynomials with integral coefficients. We prove that, up to certain admissible transformations, there is precisely one set of non-constant linear polynomials such that the product of any two of them except one combination, plus a given linear polynomial is a perfect square.

1. Introduction

Let q be a nonzero rational number. A set $\{a_1, \ldots, a_m\}$ 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 $1 \leq i < j \leq m$. This definition also makes sense in any ring instead of $\mathbb{Z}$ resp. $\mathbb{Q}$, in particular for the ring $\mathbb{Z}[x]$; in this case we shall say that $\{a_1, \ldots, a_m\}$ is a polynomial $D(q)$-m-tuple. By now this type of problem is well-known, the oldest references go back to Diophantus, Euler and Fermat; for an overview we refer e.g. to [4]. Instead of giving a complete historical overview we shall just mention a few results directly relevant for our considerations below. In [8], it was shown that for any rational q there exist infinitely many rational $D(q)$-quadruples. In this paper we study the question for which rationals q there exist infinitely many rational $D(q)$-quintuples. An affirmative answer to this question is known for rationals of the forms $q = r^2$, $q = -r^2$ and $q = -3r^2$. The result for $q = r^2$ was known already to Euler (see [17]), who proved that any $D(1)$-pair can be extended to a rational $D(1)$-quintuple (see [1, 6] for generalizations). The result for $q = -r^2$ is based on the fact that the elliptic curve associated to the quartic curve $y^2 = -(x^2 - x - 3)(x^2 + 2x - 12)$ has positive rank (see [9]), while the result for $q = -3r^2$ uses the fact that the elliptic curve $y^2 = x^3 + 42x^2 + 432x + 1296$ has positive rank (see [8]). 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 this paper, we will show that infinitely many square-free numbers q have the property that there exist infinitely many $D(q)$-quintuples. Furthermore, conjecturally the set of all square-free integers for which there exist infinitely many $D(q)$-quintuples has density $\geq 1/2$. The proof is again based on the rank of certain elliptic curves and will be given in Section 3.

Our starting point in Section 2 is the construction of a set of five linear polynomials which "almost" has the property of being a polynomial $D(q)$-quintuple, for certain linear polynomials q, in the sense that only one condition is missing. (Observe that a similar notation of "almost" has already been observed in [14, Section 5].) We will explain the

2010 *Mathematics Subject Classification.* 11D09,11C08,11G05.

Key words and phrases. Diophantine m-tuples, linear polynomials, elliptic curves, twists, rank, parity conjecture.

connection of this approach to the existence of q such that there are infinitely many $D(q)$-quintuples and then formulate and prove the result (Theorem 1). In Section 3 we shall relate the set appearing in Theorem 1 to a certain elliptic curve E and then establish the above mentioned result on the infinitude of the set of q's such that there are infinitely many $D(q)$-quintuples (Theorem 3). In the final Section 4 we shall give some explicit examples.

2. "Almost" Diophantine quintuples for linear polynomials

The result from [8] on the existence of infinitely many rational $D(q)$-quadruples for any rational q, is a corollary of results in [4] on the existence of $D(n)$-quadruples for $n \in \mathbb{Z}$. By a result of Brown [3], it was known that for $n \equiv 2 \pmod 4$ there does not exist a $D(n)$-quadruple. It is proved in [4] that if $n \not\equiv 2 \pmod 4$ and $n \notin \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there exists at least one $D(n)$-quadruple. The proof uses polynomial formulas for $D(n)$-quadruples, namely polynomial $D(n)$-quadruples where n itself is a linear polynomial with integer coefficients and the elements of the set are polynomials with small degree (typically, one constant and three quadratic, or four linear polynomials). E.g. $\{1, 9x^2 + 8x + 1, 9x^2 + 14x + 6, 36x^2 + 44x + 13\}$ is a $D(4x + 3)$-quadruple, while $\{4x, 25x + 1, 49x + 3, 144x + 8\}$ is a $D(16x + 1)$-quadruple.

A natural idea to approach the question of the existence of $D(q)$-quintuples is to construct similar sets of polynomials with five elements. However, results from [13] show that there does not exist a set of five linear polynomials with integer coefficients, not all constant, such that the product of any two of them plus a given linear polynomial is a square of a polynomial with integer coefficients, and also that there is no such set consisting of four quadratic polynomials, i.e. there is no (nontrivial) polynomial $D(n)$-quintuple with linear n consisting of linear or quadratic polynomials.

Therefore, we relax the conditions in order to get an object (that is not a polynomial m-tuple anymore) which can exist and which is still useful for our purpose (although the application will not be so straightforward). Our aim is to follow the proof of the mentioned result from [13] in order to characterize "almost" Diophantine quintuples for linear polynomials, i.e. all sets of the form $\{a_1x + b_1, \ldots, a_5x + b_5\}$ such that for given $c, d \in \mathbb{Z}, c \neq 0$ we have that $(a_ix + b_i)(a_jx + b_j) + (cx + d)$ is a square of a polynomial with integer coefficients for all $1 \leq i < j \leq 5$, except for one pair, say, without loss of generality, $(i, j) = (4, 5)$. We shall call such a set an almost $D(cx + d)$-quintuple.

There are two obvious type of transformations that we can use to produce new such sets from a given one. Let $q \in \mathbb{Z}[x]$ and $\{a_1, \ldots, a_m\}$ be a set of non-constant polynomials in $\mathbb{Z}[x]$, where for some $(i, j), i, j \in \{1, \ldots, m\}, i < j$ (we call this set S) we have $a_ia_j + q$ is a square in $\mathbb{Z}[x]$. The *admissible* transformations are given by:

Scaling: Multiply every element a_i by some $0 \neq c \in \mathbb{Z}$ to get $a'_i = ca_i$; accordingly q has to be replaced by $q' = c^2q$. If all coefficients of the a_i are divisible by $c \in \mathbb{Z}$ and q is divisible by c^2, then we can also divide through by c to get $a'_i = a_i/c$; accordingly q has to be replaced by $q' = q/c^2$.

Translation: Replace x by $ax + b$ for some $a, b \in \mathbb{Z}, a \neq 0$, to get $a'_i = a_i(ax + b)$; accordingly q has to be replaced by $q' = q(ax + b)$.

The resulting set $\{a'_1, \ldots, a'_m\}$ of non-constant polynomials in $\mathbb{Z}[x]$ has the property that $a'_ia'_j + q'$ is a square for all $(i, j) \in S$. We can also view the polynomials as elements in $\mathbb{Q}[x]$ and perform the above transformations with $a, b, c \in \mathbb{Q}$; in order to get an element in $\mathbb{Z}[x]$ we just have to cancel the denominators by multiplying with the least common multiple of them. (Below we shall use transformations over $\mathbb{Q}$ and normalize back to $\mathbb{Z}$

at the end if necessary.) The question arises if there are more admissible transformations that produce new such sets and are not covered by the two operations described above. We have the following result:

Theorem 1. *Let $q = cx + d$ and let $\{a_1, \ldots, a_5\}$ be a set of non-constant polynomials in $\mathbb{Z}[x]$ with $a_i a_j + q$ a square in $\mathbb{Z}[x]$ for all $1 \leq i < j \leq 5$, except for $(i, j) = (4, 5)$, then up to scaling and translation $\{a_1, \ldots, a_5\} = \{x, 9x + 8, 25x + 20, 4x + 2, 16x + 14\}$ and $q = 10x + 9$.*

For the proof we shall use the notation and some facts used in the proof of Theorem 1 in [13] (see Subsection 2.1 therein). We assume that the reader is familiar with this paper. We mention that the $D(10x + 9)$-quadruples $\{x, 9x + 8, 16x + 14, 25x + 20\}$ and $\{x, 4x+2, 9x+8, 25x+20\}$ already appeared as special case of the two-parametric family in [5, (11)] resp. of [4, (23)].

Proof. From [13], it follows that we may assume (by applying admissible transformations) that our quintuple has the form

$$\{A^2x, m_1^2x + 2m_1W - u, m_2^2x + 2m_2W - u, m_3^2x + 2m_3W - u, m_4^2x + 2m_4W - u\}$$

for some $A, W, u, m_1, \ldots, m_4 \in \mathbb{Z}$, while the polynomial q is of the form $A^2ux + A^2W^2$. Furthermore, if

$$(m_i^2x + 2m_iW - u)(m_j^2x + 2m_jW - u) + (A^2ux + A^2W^2)$$

is a square, then we have the following possibilities: either $|m_i - m_j| = A$ or $(2m_iW - u)(2m_jW - u) = u^2 \pm 2AWu$. Following the notation from [13], we define

$$p_i := 2m_iW - u,\ i = 1, 2, 3, 4; \quad P := u^2 - 2AWu, \quad Q := u^2 + 2AWu.$$

Because of the symmetry, we may assume that $m_1 < m_2$ and $m_3 < m_4$. We will consider several cases depending on which conditions are satisfied by m_i and m_j for corresponding pairs $(i, j) \neq (3, 4)$, and also depending on which of the two numbers m_1 and m_3 is smaller.

1) Assume first that $m_1 < m_3$. Then we have exactly three possibilities for m_2, m_3, m_4: one of them is equal to $m_1 + A$ and the other two satisfy conditions involving p_i's.

1.1) Consider first the case $m_2 = m_1 + A$. Then we may assume that $p_1p_3 = P$ and $p_1p_4 = Q$. Now $p_2p_3 \neq P$ and $p_2p_4 \neq Q$, because the m_i's are distinct integers.

There are two subcases (we may interchange the role of m_3 and m_4):
1.1.1) $m_3 = m_2 + A$ and $p_2p_4 = P$,
1.1.2) $p_2p_3 = Q$ and $p_2p_4 = P$.

1.1.1) We have $4AWu = Q-P = p_4(p_1-p_2) = -2AWp_4$, so $p_4 = -2u$. From $p_1p_4 = Q$ we get $(2m_1W - u)(-2u) = u^2 + 2AWu$, i.e. $4m_1W = u - 2AW$. Inserting this in $p_1p_3 = p_2p_4$, we get $(-u-2AW)(-u+6AW) = (-u+2AW)(-4u)$, i.e. $3u^2-4uAW+12A^2W^2 = 0$, which has no nonzero solutions.

1.1.2) From $P + Q = p_1(p_3 + p_4) = p_2(p_3 + p_4)$, since $p_1 \neq p_2$, we get $p_3 + p_4 = 0$. But then $P + Q = 2u^2 = 0$, which is a contradiction.

1.2) The next case is $m_3 = m_1+A$. Then $p_1p_2 = P$ and $p_1p_4 = Q$. Note that $p_2p_4 \neq P, Q$, thus $p_2p_3 = Q$ and $m_2 = m_4 \pm A$. We distinguish cases concerning the last two signs.

1.2.1) Assume that $m_2 = m_4 + A$. From $4AWu = Q - P = p_1(p_4 - p_2) = -2AWp_1$, we get $p_1 = -2u$. This implies $2m_1W - u = -2u$, which further yields $2m_1W = -u$. From $p_1p_4 = p_2p_3$, we get $2W(m_1m_4 - m_2m_3) = (m_1 + m_4 - m_2 - m_3)u = -2uA$. Since $m_1m_4 - m_2m_3 = -A(m_1 + m_2)$, we get that $u = W(m_1 + m_2)$. Thus $m_1 + m_2 = -2m_1$, i.e. $m_2 = -3m_1$. From $p_1p_2 = P$, we get $-2u(2m_2W - u) = u^2 - 2AWu$, and this implies

$2AW = 5u$. Hence, $m_1 = -A/5$, $m_2 = 3A/5$, $m_3 = 4A/5$, $m_4 = -2A/5$. Thus, we obtain the set

$$\left\{A^2x, \frac{1}{25}A^2x - \frac{2}{5}AW - \frac{2}{5}AW, \frac{9}{25}A^2x + \frac{6}{5}AW - \frac{2}{5}AW, \frac{16}{25}A^2x + \frac{8}{5}AW - \frac{2}{5}AW, \right.$$
$$\left. \frac{4}{25}A^2x - \frac{4}{5}AW - \frac{2}{5}AW\right\}$$

which is an almost $D(A^2(\frac{2}{5}AW)x + A^2W^2)$-quintuple. By translating $\frac{1}{25}A^2x$ to x and substituting, $\alpha := \frac{1}{5}AW$, we get the set

$$\{25x, x - 4\alpha, 9x + 4\alpha, 16x + 6\alpha, 4x - 6\alpha\}, \tag{1}$$

which is an almost $D(50\alpha x + 25\alpha^2)$-quintuple.

1.2.2) Assume now that $m_2 = m_4 - A$. We get $p_1 = 2u$ and $2m_1W = 3u$. The equality $p_1p_4 = p_2p_3$ gives $2AW(m_1 - m_2) = 2W(m_1m_4 - m_2m_3) = (m_1 + m_4 - m_2 - m_3)u = 0$, which is a contradiction.

2) It remains to consider the case when $m_3 < m_1$. We consider the different possibilities for m_1 and m_2.

2.1) Assume that $m_1 = m_3+A$. Then $p_2p_3 = P$ (resp. Q). Further we have the following subcases:

2.1.1) $m_2 = m_1 + A$, $m_4 = m_2 + A$ and $p_1p_4 = P$ (resp. Q),
2.1.2) $m_2 = m_1 + A$, $m_4 = m_2 + A$ and $p_1p_4 = Q$ (resp. P),
2.1.3) $p_1p_2 = Q$ (resp. P), $m_4 = m_2 \pm A$ and $p_1p_4 = P$ (resp. Q),
2.1.4) $p_1p_2 = Q$ (resp. P), $m_4 = m_2 - A$ and $m_4 = m_1 + A$.

2.1.1) From $p_2p_3 = p_1p_4$, we have $4W(m_2m_3-m_1m_4) = 2(m_2+m_3-m_1-m_4)u$, which gives $W(2m_3+3A) = u$. Inserting this in $p_2p_3 = u^2 \pm 2AWu$, we get $4W^2m_3(m_3+2A) = \pm 2AWu + 2uW(2m_3 + 2A) = 2W^2(2m_3 + 3A)(2m_3 + 2A \pm A)$. For the + sign we get, $2m^3 + 8Am_3 + 9A^2 = 0$, while for the − sign we get $2m_3^2 + 2Am_3 + 3A^2 = 0$, and both equations have no nonzero integer solutions.

2.1.2) From $p_2p_3 - p_1p_4 = \mp 4AWu$, we get $4W^2(m_2m_3 - m_1m_4) = 2(m_2 + m_4 - m_1 - m_4) \mp 4Au$. In the case of the − sign, this leads to $AW(m_1 + m_2) = 0$. But this means that $m_1 = -A/2$, $m_2 = A/2$, $m_3 = -3A/2$, $m_4 = 3A/2$ and $u = 0$, a contradiction.

For the + sign, we obtain $W(2m_3 + 3A) = 2u$. Inserting this in $p_2p_3 = u^2 - 2AWu$ gives $4W^2m_3(m_3 + 2A) = 2uW(2m_3 + A) = W^2(2m_3 + 3A)(2m_3 + A)$ and $AW = 0$, a contradiction.

The case **2.1.3)** is equivalent to the case 1.2) (by taking $-A$ instead of A).

2.1.4) From $4AWu = Q - P = p_2(p_1 - p_3) = p_2 2AW$, we get $p_2 = 2u$ or $p_2 = -2u$ (with interchanged role of P and Q). This implies $2m_2W = 3u$ or $2m_2W = -u$. Now $(2m_1W - u)2u = u^2 + 2AWu$ gives $2W(2m_1 - A) = 3u$ or $(2W(2m_1 - A) = u$. The first case gives $m_2 = 2m_1 - A$, while the second gives $m_2 = -2m_1 + A$. We also have $m_2 = m_1 + 2A$, which gives in the first case $m_1 = 3A$, $m_2 = 5A$, $m_3 = 2A$, $m_4 = 4A$, $u = 10AW/3$, and in the second case $m_1 = -A/3$, $m_2 = 5A/3$, $m_3 = -2A/3$, $m_4 = 4A/3$, $u = -10AW/3$.

Thus we get in the first case the set

$$\left\{A^2x, 9A^2x + 6AW - \frac{10}{3}AW, 25A^2x + 10AW - \frac{10}{3}AW, 4A^2x + 4AW - \frac{10}{3}AW, \right.$$
$$\left. 16A^2x + 8AW - \frac{10}{3}AW\right\}$$

which is an almost $D(A^2(\frac{10}{3}AW)x + A^2W^2)$-quintuple. By translating A^2x to x and substituting $\alpha := \frac{1}{3}AW$, we get the set

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

which is an almost $D(10\alpha x + 9\alpha^2)$-quintuple.

In the second case we get the set

$$\left\{A^2x, \frac{1}{9}A^2x - \frac{2}{3}AW + \frac{10}{3}AW, \frac{25}{9}A^2x + \frac{10}{3}AW + \frac{10}{3}AW, \frac{16}{9}A^2x - \frac{8}{3}AW + \frac{10}{3}AW, \right.$$
$$\left. \frac{4}{9}A^2x + \frac{4}{3}AW + \frac{10}{3}AW\right\}$$

which is an almost $D(A^2(-\frac{10}{3}AW)x + A^2W^2)$-quintuple. By translating $\frac{1}{9}A^2x$ to x and substituting $\alpha := \frac{1}{3}AW$, we get the set

$$\{9x, x + 8\alpha, 25x + 20\alpha, 4x + 14\alpha, 16x + 2\alpha\} \tag{3}$$

which is an almost $D(-90\alpha x + 9\alpha^2)$-quintuple.

2.2) The next possibility we have to discuss is $m_2 = m_3 + A$. Then $p_1p_3 = P$, $p_1p_2 = Q$, $m_4 = m_1 \pm A$, $p_1p_4 = P$. We see that this case is equivalent to 2.1.3).

2.3) The last possibility is that $p_1p_3 = P$ and $p_2p_3 = Q$. We have the following possibilities for the relations between m_1, m_2, m_4:
2.3.1) $m_2 = m_1 + A$, $p_1p_4 = Q$ and $p_2p_4 = P$,
2.3.2) $m_2 = m_1 + A$, $p_1p_4 = Q$ and $m_4 = m_2 + A$.

The case 2.3.1) is identical to the case 1.1.2), while the case 2.3.2) is equivalent to the case 1.1.1).

So far we have obtained three quintuples (1), (2) and (3) with the desired property. We will now show that they are equivalent in the sense that they can be obtained one from the other by admissible transformations. Take first the almost $D(50\alpha x + 25\alpha^2)$-quintuple $\{25x, x - 4\alpha, 9x + 4\alpha, 16x + 6\alpha, 4x - 6\alpha\}$. By translating x to $5x + 4\alpha$, we get the almost $D(250\alpha x + 225\alpha^2)$-quintuple $\{125x + 100\alpha, 5x, 45x + 40\alpha, 80x + 70\alpha, 20x + 10\alpha\}$, and by dividing all of its elements by 5 and correspondingly q by 25, we get exactly the set (2). Take now the almost $D(-90\alpha x+9\alpha^2)$-quintuple $\{9x, x+8\alpha, 25x+20\alpha, 4x+14\alpha, 16x+2\alpha\}$. By translating x to $-9x - 8\alpha$, we get the almost $D(810\alpha x + 729\alpha^2)$-quintuple $\{-81x - 72\alpha, -9x\alpha, -225x - 180\alpha, -36x - 18\alpha, -144x - 126\alpha\}$, and by dividing all of its elements by -9 and correspondingly q by 81, we get exactly the set (2). Furthermore, by dividing the elements of (2) by α, we get that all quintuples with the desired property can be obtained from the almost $D(10x + 9)$-quintuple $\{x, 9x + 8, 25x + 20, 4x + 2, 16x + 14\}$ by the admissible transformations. This proves the assertion. □

3. Twists of an elliptic curve

In the previous section we proved that for a rational number x the sets $\{x, 4x + 2, 9x + 8, 25x + 20\}$ and $\{x, 9x + 8, 16x + 14, 25x + 20\}$ are rational $D(10x + 9)$-quadruples. Therefore, the set

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

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

$$(4x + 2)(16x + 14) + 10x + 9 = y^2 \tag{4}$$

for a $y \in \mathbb{Q}$. Inserting $y = 8x + t$ in (4), we obtain

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

Thus, we have proved:

Theorem 2. *The set*

$$\{t^2 - 37, 4t^2 - 32t + 48, 9t^2 - 128t + 451, 16t^2 - 224t + 780, 25t^2 - 320t + 1035\} \tag{5}$$

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 on using Theorem 2 we can get a rational $D(q)$-quintuple. If there exist rationals $s \neq 0$ and t such that

$$4(8 - t)(5t - 32)(8t - 49) = qs^2, \tag{6}$$

then by dividing all elements of (5) by s, we exactly get a $D(q)$-quintuple. The equation (6) with $q = 1$ defines an elliptic curve E 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) given by (6). 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 substitution $t = -x/40 + 49/8, s = y$, we get an equation of the curve E in short Weierstrass form

$$E\colon\ y^2 = x(x + 11)(x + 75) = x^3 + 86x^2 + 825x. \tag{7}$$

The curve E has discriminant $D = 2^{16}3^25^411^2$ and conductor $C = 330 = 2 \cdot 3 \cdot 5 \cdot 11$. Its minimal model is given by $y^2 + xy = x^3 + x^2 - 102x + 324$. Furthermore, 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

$$E_q\colon\ qy^2 = x^3 + 86x^2 + 825x. \tag{8}$$

If q is of the form

$$q = uv(u^2 + 86uv + 825v^2), \tag{9}$$

for integers u, v, then there is a point $(u/v, 1/v^2)$ of infinite order on the curve E_q. 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. Indeed, 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 (9) (see e.g. [16]).

Assuming the Parity Conjecture for all twists of E, we can give a precise description of those q's for which the rank of its q-twist is odd (and therefore positive). We remind the reader that the Parity Conjecture (for E) says that the rank of the Mordell-Weil group of E is equal to the order of vanishing of the associated L-function $L(E, s)$ at $s = 1$ modulo 2. This statement is of course implied by the Birch and Swinerton-Dyer Conjecture. It is known that if the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ of E is finite, then the Parity Conjecture holds true for E (cf. [18]). The Parity Conjeture implies that for a square-free integer q relative prime to twice the conductor C of E, the (Mordell-Weil) ranks of E and E_q are equal modulo 2 if and only if $\chi_q(-C) = 1$, where χ_q is the quadratic

Dirichlet character associated to $\mathbb{Q}(\sqrt{q})$ (cf. [16, p. 2]). Finally, we 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 $N \to \infty$. For us it would be sufficient to get hold on those twists for which the rank is positive; the Parity Conjecture implies that the number of these square-free q's with $|q| \leq N$ is $\geq 6N/\pi^2$ (see [19]). We have the following theorem:

Theorem 3. *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* (7) *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 settled above. 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 $\mathbb{Q}(\sqrt{q})$ (see e.g. [16]). 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 (7). 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 $2^k|g|N$ for an integer k (actually, $k \in \{0, 3, 4\}$). 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) ($q \equiv i \pmod{1320}$, $i = 1, 7, 9, 10, 11, 18, 21, 22, 23, \; 30, \ldots, 1315, 1319$) satisfy the condition that the rank of the q-twist is odd (we consider only those classes not divisible by 4, since we are interested in square-free numbers). This proves the theorem. □

As mentioned above, it is sufficient for us to find q's such that the twist E_q has rank ≥ 1. It is worth mentioning 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.

4. Some examples

The smallest positive integer q 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 (6). From Theorem 2 we obtain the rational $D(7)$-quintuple

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

By multiplying all elements of this quintuple by 40, we get an integer $D(11200)$-quintuple.

The greatest negative integer with the same property is $q = -2$. The (-2)-twist has rank 1 and the generator of the Mordell-Weil group is $(x, y) = (-297/2, 3465/4)$. It induces the point $(t, s) = (787/80, 693/16)$ on (6). From Theorem 2 we obtain the following rational $D(-2)$-quintuple

$$\left\{\frac{11593}{8400}, \frac{5833}{2100}, \frac{4059}{2800}, \frac{1513}{525}, \frac{2377}{336}\right\}.$$

By multiplying all elements of this quintuple by 8400, we get an integer $D(-141120000)$-quintuple.

We mention that the smallest positive integer n for which the construction from Theorem 2 gives an integer $D(n)$-quintuple is $n = 1309$ in which case we get the $D(1309)$-quintuple $\{2, 30, 106, 186, 290\}$, while the greatest negative integer with the same property is $n = -299$ by means of the $D(-299)$-quintuple $\{14, 22, 30, 42, 90\}$. Going further in this direction one may ask what the least positive integer n_1 and what the greatest negative integer n_2 is, for which there exists a Diophantine quintuple with the property $D(n_i)$, $i = 1, 2$. It is known that $n_1 \leq 256$ and $n_2 \geq -255$, since the sets $\{1, 33, 105, 320, 18240\}$ and $\{5, 21, 64, 285, 6720\}$ have the property $D(256)$, and the set $\{8, 32, 77, 203, 528\}$ has the property $D(-255)$ (see [6, 7]). We also mention the famous conjecture, motivated by the result of Baker and Davenport [2] on the nonextendibility of Fermat's example of a $D(1)$-quadruple given by $\{1, 3, 8, 120\}$, that there does not exist a $D(1)$-quintuple. (In [10] it has been proved that there are only finitely many $D(1)$-quintuples and that there is no $D(1)$-sextuples.) In [12], it has been proved that there does not exist a $D(-1)$-quintuple. So, in above terminology, we know that $n_2 \leq -3$.

Let us mention that several rational $D(q)$-sextuples are known (see [15, 11]), but in all known examples q is a perfect square.

References

[1] J. Arkin, V. E. Hoggatt and E. G. Strauss, *On Euler's solution of a problem of Diophantus*, Fibonacci Quart. **17** (1979), 333–339.

[2] 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.

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

[4] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arith. **65** (1993), 15–27.

[5] A. Dujella, *Some polynomial formulas for Diophantine quadruples*, Grazer Math. Ber. **328** (1996), 25–30.

[6] A. Dujella, *On Diophantine quintuples*, Acta Arith. **81** (1997), 69–79.

[7] A. Dujella, *A problem of Diophantus and Pell numbers*, Application of Fibonacci Numbers, Vol. **7** (G. E. Bergum, A. N. Philippou, A. F. Horadam, eds.), Kluwer, Dordrecht, 1998, pp. 61–68.

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

[9] A. Dujella, *An extension of an old problem of Diophantus and Euler. II*, Fibonacci Quart. **40** (2002), 118–123.

[10] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.
[11] A. Dujella, *Rational Diophantine sextuples with mixed signs*, Proc. Japan Acad. Ser. A Math. Sci. **85** (2009), 27–30.
[12] A. Dujella and C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. **71** (2005), 33–52.
[13] A. Dujella, C. Fuchs and P. G. Walsh, *Diophantine m-tuples for linear polynomials. II. Equal degrees*, J. Number Theory **120** (2006), 213–228.
[14] A. Dujella and V. Petričević, *Strong Diophantine triples*, Experiment. Math. **17** (2008), 83–89.
[15] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), 195–203.
[16] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.
[17] T. L. Heath, Diophantus of Alexandria. A Study in the History of Greek Algebra. With a supplement containing an account of Fermat's theorems and problems connected with Diophantine analysis and some solutions of Diophantine problems by Euler, Powell's Bookstore, Chicago, 2003.
[18] P. Monsky, *Generalizing the Birch-Stephens theorem. I. Modular curves*, Math. Z. **221** (1996), 415–420.
[19] A. Silverberg, *The distribution of ranks in families of quadratic twists of elliptic curves*, Ranks of Elliptic Curves and Random Matrix Theory (J. B. Conrey, D. Farmer, F. Mezzadri, N. C. Snaith, eds.), London Math. Soc. Lect. Note Series **341**, Cambridge Univ. Press, Cambridge, 2007, pp. 171–176.

Andrej Dujella
Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb
Croatia
Email: duje@math.hr

Clemens Fuchs
Department of Mathematics
ETH Zurich
Rämistrasse 101
8092 Zürich
Switzerland
Email: clemens.fuchs@math.ethz.ch