Strong Diophantine Triples

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

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

Diophantine m-tuples

A set $\{a_1, a_2, \dots, a_m\}$ of m non-zero integers (rationals) is called a (rational) Diophantine m-tuple if $a_i \cdot a_j + 1$ is a perfect square for all $1 \le i < j \le m$. Diophantus of Alexandria found a rational Diophantine quadruple $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$, while the first Diophantine quadruple in integers, the set $\{1, 3, 8, 120\}$, was found by Fermat. Euler was able to add the fifth positive rational, $777480/8288641$, to the Fermat's set. Euler's construction has been generalized in [2], where it was shown that every rational Diophantine quadruple, the product of whose elements is not equal to 1, can be extended to a rational Diophantine quintuple. Recently, Gibbs [6] found several examples of rational Diophantine sextuples. The first one was

$$\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}.$$

A famous conjecture is that there does not exist a Diophantine quintuple (in non-zero integers) (see e.g. [7]). In 1969, Baker and Davenport [1] proved that the Fermat's set $\{1, 3, 8, 120\}$ cannot be extended to a Diophantine quintuple. In 1998, Dujella and Pethő [4] proved that the pair $\{1, 3\}$ cannot be extended to a Diophantine quintuple. Recently, the first author proved in [3] that there does not exist a Diophantine sextuple and there are only finitely many Diophantine quintuples.

Strong Diophantine m-tuples

Note that in the definition of (rational) Diophantine m-tuples we exclude $i = j$, i.e. the condition $a_i^2 + 1$ is a square. It is obvious that for integers, such condition has no sense.

Definition 1 *A set of m nonzero rationals $\{a_1, a_2, \dots, a_m\}$ is called* a strong Diophantine m-tuple *if $a_i \cdot a_j + 1$ is a perfect square for all $i, j = 1, \dots, m$.*

It seems to be very hard to find an absolute upper bound for the size of strong (rational) Diophantine tuples. The first strong Diophantine triple, the set

$$\left\{\frac{1976}{5607}, \frac{3780}{1691}, \frac{14596}{1197}\right\}$$

was found by the first author in 2000. No example of a strong Diophantine quadruple is known. The problem of extension of given strong Diophantine triple $\{a_1, a_2, a_3\}$ to a quadruple $\{a_1, a_2, a_3, x\}$, leads to the hyperelliptic curve

$$y^2 = (x^2 + 1)(a_1 x + 1)(a_2 x + 1)(a_3 x + 1)$$

of genus $g = 2$. Although the examples from last section might suggest that the discovering of strong Diophantine quadruples is not unrealistic, the existence of a strong Diophantine quintuple is very unlikely.

We have performed a search for more examples of strong Diophantine triples in various regions. We have found more that 50 such triples with at least two elements with relatively small numerators and denominators. The analysis of the special properties of some of these examples leads us to the following theorem.

Theorem 1 *There exist infinitely many strong Diophantine triples of positive rational numbers.*

We have found two different proofs of Theorem 1, i.e. two different constructions of infinitely many strong Diophantine triples (and we show that moreover infinitely many of them have positive elements). Both constructions are based on some elliptic curves over $\mathbb{Q}$ with positive rank.

Associated elliptic curves

To a non-zero rational a, we associate the elliptic curve

$$E_a: \quad y^2 = (x^2 + 1)(ax + 1). \qquad (1)$$

It has a rational point $T = [-1/a, 0]$, which is the torsion point of order 2, and another rational point $P = [0, 1]$, which is (in general) a point of infinite order. Indeed, by considering the coordinates of the point

$$3P = \left[\frac{8a(a^2+4)}{(a^2-4)^2}, \frac{(3a^2+4)(a^4+24a^2+16)}{(a^2-4)^3}\right],$$

using Lutz-Nagell theorem, it is easy to check that P has infinite order, except for $a = \pm 2$, when it has order 3. Note that $P + T = [a, -a^2 - 1]$.

We may consider the elliptic surface $\mathcal{E}$ associated with the family of curves E_a. Using Shioda's formula [8], we find that rank $\mathcal{E}(\mathbb{C}(a)) = 1$. Since we already know that $[0, 1]$ is a point of infinite order on $\mathcal{E}(\mathbb{Q}(a))$, we conclude that also rank $\mathcal{E}(\mathbb{Q}(a)) = 1$.

Strong Diophantine pairs

Assume now that $a^2 + 1$ is a perfect square. Then all points of the form mP or $mP + T$ satisfy the additional condition that the both factors of the cubic polynomial in (1) are perfect squares (it suffices to check that this condition is fulfilled for T, P and $P + T$). Therefore, the first coordinates of these points induce pairs $\{a, b\}$ that are strong Diophantine pairs. If we parametrize a by $a = 2t/(t^2 - 1)$, then we may take e.g.

$$b = \frac{-(t^2+t-1)(t^2-t-1)}{2t(t^2-1)}, \qquad b = \frac{t^6-1}{2t^3},$$
$$b = \frac{4t(t^2-1)(t^4-t^2+1)}{(t^2+t-1)^2(t^2-t-1)^2}, \qquad b = \frac{2t(3t^4-t^8-1)}{(t^2-1)(t^4+t^2+1)^2},$$

which are respectively the first coordinates of the points $2P$, $2P + T$, $3P$, $3P + T$.

Strong Diophantine triples

Assume now that $\{a, b, c\}$ is an arbitrary strong Diophantine triple. Then the points with the first coordinates b and c also belong to $E_a(\mathbb{Q})$. Denote these points by B and C. Let e and f be the first coordinates of the points $B + T$ and $C + T$, respectively, i.e. $e = \frac{a-b}{ab+1}$, $f = \frac{a-c}{ac+1}$. It is easy to verify that $\{a, e, f\}$ is also a strong Diophantine triple. We can interchange the role of a, b, c in the above construction. In that way, starting with one strong Diophantine triple $\{a, b, c\}$, we obtain (in general) another three strong Diophantine triples:

$$\left\{a, \frac{a-b}{ab+1}, \frac{a-c}{ac+1}\right\}, \quad \left\{b, \frac{b-a}{ab+1}, \frac{b-c}{bc+1}\right\}, \quad \left\{c, \frac{c-a}{ac+1}, \frac{c-b}{bc+1}\right\}.$$

Note that among these four triples exactly two have all positive elements.

Example 1 *Starting with the triple*

$$\left\{\frac{140}{51}, \frac{187}{84}, -\frac{427}{1836}\right\},$$

we obtain three new strong Diophantine triples:

$$\left\{\frac{140}{51}, \frac{2223}{30464}, \frac{278817}{33856}\right\}, \quad \left\{\frac{187}{84}, -\frac{2223}{30464}, \frac{15168}{2975}\right\}, \quad \left\{\frac{427}{1836}, \frac{278817}{33856}, \frac{15168}{2975}\right\}.$$

However, it should be observed that the four strong Diophantine triples obtained with the above construction are not always necessarily distinct.

Example 2 *If we start with the triple*

$$\left\{\frac{1976}{5607}, \frac{3780}{1691}, \frac{14596}{1197}\right\},$$

then the only new triple obtained with the above construction is

$$\left\{\frac{1976}{5607}, -\frac{19853044}{16950717}, -\frac{3780}{1691}\right\}.$$

Note that the strong Diophantine pair $\{a, b\} = \{1976/5607, 3780/1691\}$ has the additional property that $a \cdot (-b) + 1$ is also a perfect square.

Lemma 1 *Each strong Diophantine pair $\{a, b\}$ with the property that $1 - ab$ is a perfect square can be extended to a strong Diophantine triple.*

Proof. We take $c = \frac{a+b}{1-ab}$, and we claim that $\{a, b, c\}$ is a strong Diophantine triple. Indeed, $ac + 1 = \frac{a^2+1}{1-ab}$, $bc + 1 = \frac{b^2+1}{1-ab}$ and $c^2 + 1 = \frac{(a^2+1)(b^2+1)}{(1-ab)^2}$ are perfect squares. ❑

Note that if $c = \frac{a+b}{1-ab}$, then $\frac{c-a}{ac+1} = b$ and $\frac{c-b}{bc+1} = a$, and therefore we obtain only two different triples with our construction. In terms of the elliptic curve E_c, in this case the addition of the 2-torsion point just interchange the points with the first coordinates a and b.

We can show that there exist infinitely many strong Diophantine pairs $\{a, b\}$ with the additional property that $1 - ab$ is also a perfect square. Hence, we want to find non-zero rationals a, b such that

$$a^2 + 1, \quad b^2 + 1, \quad ab + 1, \quad 1 - ab \qquad (2)$$

are perfect squares.

Thus, the question is how we can fulfill the four conditions from (2). Let us fix $\alpha := a \cdot b$ such that $1 + \alpha$ and $1 - \alpha$ are perfect squares. The condition $b^2 + 1 = \square$ has the parametric solution $b = 2t/(t^2 - 1)$. Inserting this into the condition $a^2 + 1 = \square$, we obtain the condition

$$\alpha^2(t^2 - 1)^2 + (2t)^2 = s^2. \qquad (3)$$

The quartic (3) can be transformed in the standard way into an elliptic curve in Weierstrass form. If such curve has positive rank, we will obtain infinitely many pairs $\{a, b\}$ with desired property. Let us use the pairs from Example 2. For $\alpha = 1617/10744 \cdot 15168/2975 = 5544/7225$, we obtain the curve

$$y^2 + xy = x^3 - 43024332146390x - 32779590846716529900.$$

Using the specialized programs, like *MWRANK* or *APECS*, we can compute the rank of this curve. We obtain that the rank is equal to 1 (with the generator $[-802370, -1106521940]$, and the torsion group isomophic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$). Therefore, we proved the following lemma.

Lemma 2 *There exist infinitely many strong Diophantine pairs $\{a, b\}$ with the property that $1 - ab$ is a perfect square.*

Lemmas 1 and 2 imply that there exist infinitely many strong Diophantine triples, and by the remark after Lemma 1 we also know that there exist infinitely many such triples with positive elements. Thus, we actually proved Theorem 1. ❑

We list some of the triples obtained with this construction

$$\left\{\frac{54619093071}{22098986000}, \frac{544519015040}{1753879766391}, \frac{10782864028595651621676\,1}{9017829641758970738160}\right\},$$

$$\left\{\frac{54619093071}{22098986000}, -\frac{544519015040}{1753879766391}, \frac{837620041057510173367 61}{685000991645569883138 40}\right\},$$

$$\left\{\frac{144763558601204723585791 0848}{92775448621813890386857 6025}, \frac{504261850156211968926214263}{1025408540091866792066020184}, \frac{1161361740957008922125901324903233342330112123673647}{1316716087580099326514596607432530053419824914 86296}\right\}.$$

Example 3 *Consider the strong Diophantine triple*

$$\left\{\frac{364}{627}, \frac{475}{132}, -\frac{132}{475}\right\}.$$

It has the form $\{a, b, -1/b\}$. Our construction gives now only one new triple $\left\{\frac{364}{627}, -\frac{297}{304}, \frac{304}{297}\right\}$ (of the same form). In general, we obtain one new triple $\left\{a, \frac{a-b}{ab+1}, \frac{1+ab}{b-a}\right\}$ (and no triples with positive elements). In terms of the elliptic curve E_b, the point with the first coordinate $c = -1/b$ is the 2-torsion point, so in this case the addition of the 2-torsion point gives the point at infinity.

We can show that there exist infinitely many strong Diophantine triples of the form $\{a, b, -1/b\}$, and that from every such triple we can obtain a triple with positive elements. This gives the second proof of Theorem 1 (see [5] for details).

"Almost" strong Diophantine quadruples

It is not known whether there exists any strong Diophantine quadruple. Such a set has to satisfy 10 conditions of the form $xy + 1$ is a square. However, we were able to find quadruples (with relatively small numerators and denominators) satisfying 9 of these 10 conditions. In Example 1, we considered the strong Diophantine triple $\left\{\frac{140}{51}, \frac{187}{84}, -\frac{427}{1836}\right\}$. Perhaps surprisingly, we were able to find another extension of the pair $\{140/51, 187/84\}$ to a strong Diophantine triple, namely the triple $\left\{\frac{140}{51}, \frac{187}{84}, -\frac{7200}{20111}\right\}$. Therefore, we obtained an "almost" strong Diophantine quadruple

$$\left\{\frac{140}{51}, \frac{187}{84}, -\frac{427}{1836}, -\frac{7200}{20111}\right\},$$

which satisfies almost all conditions for a strong Diophantine quadruple. The only missing condition is that $(-\frac{427}{1836}) \cdot (-\frac{7200}{20111}) + 1$ is not a perfect square.

Using the construction described before Example 1, we can find another example with the same property (and with positive elements):

$$\left\{\frac{140}{51}, \frac{2223}{30464}, \frac{278817}{33856}, \frac{3182740}{17661}\right\}.$$

In this case, the only missing condition is that $\frac{278817}{33856} \cdot \frac{3182740}{17661} + 1$ is not a perfect square.

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

[3] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

[4] A. Dujella and A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) **49** (1998), 291–306.

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

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

[7] R. K. Guy, Unsolved Problems in Number Theory, 3rd edition, Springer-Verlag, New York, 2004, Section D29.

[8] T. Shioda, *On the Mordell - Weil lattices*, Comment. Math. Univ. St. Pauli **39** (1990), 211–240.