AN EXTENSION OF AN OLD PROBLEM OF DIOPHANTUS AND EULER. II

Andrej Dujella

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

Diophantus found three rationals $\frac{3}{10}$, $\frac{21}{5}$, $\frac{7}{10}$ with the property that the product of any two of them increased by the sum of those two gives a perfect square (see [5, pp. 85–86, 215–217]), and Euler found four rationals $\frac{65}{224}$, $\frac{9}{224}$, $\frac{9}{56}$, $\frac{5}{2}$ with the same property (see [4, pp. 518–519]).

A set $\{x_1, x_2, \ldots, x_m\}$ of m rationals such that $x_i x_j + x_i + x_j$ is a perfect square for all $1 \le i < j \le m$ we will call *an Eulerian m-tuple.*

In [8] we found the Eulerian quintuple

$$\{-\frac{27}{40}, \frac{17}{8}, \frac{27}{10}, 9, \frac{493}{40}\}. \tag{1}$$

This example leads us to the following questions: Is there any Eulerian quintuple consisting of positive rationals (this would be more in the style of Diophantus) and are there infinitely many such quintuples. In the present paper we give affirmative answers to the both questions.

Let us mention that it is not known whether there exists any Eulerian quadruple consisting of integers. In [3, 10, 12] it was proved that some particular Eulerian triples cannot be extended to an integer quadruple, and in [7] it was proved that the Eulerian pair $\{0, 1\}$ cannot be extended to an integer quadruple.

Let q be a rational number. A set $\{a_1, a_2, \ldots, a_m\}$ of m non-zero rationals is called *a Diophantine m-tuple with the property $D(q)$* if $a_i a_j + q$ is a perfect square for all $1 \le i < j \le m$ (see [6]). It is clear that $\{x_1, x_2, \ldots, x_m\}$ is an Eulerian m-tuple iff $\{x_1 + 1, x_2 + 1, \ldots, x_m + 1\}$ is a Diophantine m-tuple with the property $D(-1)$.

In [8] we proved that the set

$$\begin{gathered}\{\tfrac{1}{3}(x^2+6x-18)(-x^2+2x+2),\ \tfrac{1}{3}x^2(x+5)(-x+3),\ (x-2)(5x+6),\\ \tfrac{1}{3}(x^2+4x-6)(-x^2+4x+6),\ 4x^2\}\end{gathered} \tag{2}$$

has the property $D(\frac{16}{9}x^2(x^2-x-3)(x^2+2x-12))$. From (2) for $x=\frac{5}{2}$ we obtain the Eulerian quintuple (1).

Consider the quartic curve

$$Q: \quad y^2 = -(x^2-x-3)(x^2+2x-12)\,.$$

We have a rational point $(\frac{5}{2},\frac{3}{4})$ on Q. Using the construction from [1], we find that, with the substitution

$$x=\frac{63s+10t+2619}{18s+4t+2403}, \quad y=\frac{24s^3-6777s^2-12t^2-34749t+54898479}{(18s+4t+2403)^2}, \tag{3}$$

Q is birationally equivalent to the elliptic curve

$$\begin{aligned} E: \quad t^2 &= s^3-18981s-1001700 \\ &= (s-159)(s+75)(s+84). \end{aligned}$$

Using the program package SIMATH (see [14]) we obtain the following information about curve E: $E(\mathbf{Q})_{\rm tors}\simeq \mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$, $E(\mathbf{Q})_{\rm tors}=\{\mathcal{O},A=(159,0),B=(-75,0),C=(-84,0)\}$, $\operatorname{rank}E(\mathbf{Q})=1$, $E(\mathbf{Q})/E(\mathbf{Q})_{\rm tors}=<P>$, where $P=(2103,-96228)$. The author is grateful to the referee for the observation that the minimal equation for E is $v^2=u^3-u^2-234u-1296$. It is curve 1246E1 in John Cremona's online tables, which confirm that the rank of E is equal to 1.

As a direct consequence of the fact that $\operatorname{rank}E(\mathbf{Q})=1$ we conclude that there are infinitely many rational points on Q. By (2) we obtain infinitely many Diophantine quintuples with the property $D(-\frac{16}{9}x^2y^2)$, and multiplying elements of these quintuples by $\frac{3}{4xy}$ we obtain quintuples with the property $D(-1)$. Therefore we proved

Theorem 1 *There exist infinitely many Diophantine quintuples with the property $D(-1)$.*

Corollary 1 *There exist infinitely many Eulerian quintuples.*

Next question is which points (s,t) on $E(\mathbf{Q})$ induce Eulerian quintuples with positive elements or, equivalently, Diophantine quintuples with the property $D(-1)$, whose elements are > 1.

Therefore, we would like to find the points (x,y) on Q such that the five rationals

$$\tfrac{(x^2+6x-18)(-x^2+2x+2)-4xy}{4xy}, \quad \tfrac{x(x+5)(-x+3)-4y}{4y}, \quad \tfrac{3(x-2)(5x+6)-4xy}{4xy},$$
$$\tfrac{(x^2+4x-6)(-x^2+4x+6)-4xy}{4xy}, \quad \tfrac{3x-y}{y}$$

are all positive. Let denote these five expressions by $R_1(x,y),\dots,R_5(x,y)$. First of all, from $(x^2-x-3)(x^2+2x-12)=-y^2\le 0$, it follows

$$x \in [-1-\sqrt{13}, \frac{1-\sqrt{13}}{2}] \cup [\frac{1+\sqrt{13}}{2}, -1+\sqrt{13}]. \tag{4}$$

Here,

$$-1-\sqrt{13} \approx -4.605551275464, \quad \tfrac{1-\sqrt{13}}{2} \approx -1.302775637732$$
$$\tfrac{1+\sqrt{13}}{2} \approx 2.302775637732, \quad -1+\sqrt{13} \approx 2.605551275464.$$

Set $\alpha = \frac{1+\sqrt{13}}{2}$ and $\beta = \frac{-1+\sqrt{13}}{2}$. Then condition (4) may be written in the form

$$x \in [-2\alpha, -\beta] \cup [\alpha, 2\beta].$$

Assume first that $y > 0$. Then we find (using Mathematica) that $R_1(x,y) > 0$ iff $x \in \langle \alpha, x^{(1)}\rangle \cup \langle x^{(2)}, 2\beta\rangle$, where

$$x^{(1)} \approx 2.306300513595, \quad x^{(2)} \approx 2.601569034318;$$

$R_2(x,y) > 0$ iff $x \in \langle \alpha, 2\beta\rangle$; $R_3(x,y) > 0$ iff $x \in \langle \alpha, 2\beta\rangle$; $R_4(x,y) > 0$ iff $x \in \langle \alpha, 2\beta\rangle$; $R_5(x,y) > 0$ iff $x \in \langle \alpha, 2\beta\rangle$.

Assume now that $y < 0$. Then we find that $R_1(x,y) > 0$ iff $x \in \langle -2\alpha, -\beta\rangle$; $R_2(x,y) > 0$ iff $x \in \langle -2\alpha, x^{(3)}\rangle \cup \langle -3, -\beta\rangle$, where

$$x^{(3)} \approx -4.482360405707;$$

$R_3(x,y) > 0$ iff $x \in \langle -2\alpha, -2\rangle \cup \langle x^{(4)}, -\beta\rangle$, where

$$x^{(4)} \approx -1.338580448007;$$

$R_4(x,y) > 0$ iff $x \in \langle -2\alpha, -\beta\rangle$; $R_5(x,y) > 0$ iff $x \in \langle -2\alpha, -3\rangle \cup \langle -2, -\beta\rangle$.

Summarizing these computations we may write that $R_i(x,y) > 0$ for $i = 1,\ldots,5$ iff

$$x \in \langle \alpha, x^{(1)} \rangle \cup \langle x^{(2)}, 2\beta \rangle,\ y > 0 \quad \text{or} \quad x \in \langle -2\alpha, x^{(3)} \rangle \cup \langle x^{(4)}, -\beta \rangle,\ y < 0. \tag{5}$$

We can see also that we have only three possibilities for the signs of $R_i(x,y)$, $i = 1,\ldots,5$. Namely, we may have zero, one or five negative numbers among them. This is not surprising. Indeed, it is a consequence of the following simple fact.

Proposition 1 *There does not exist an Eulerian triple* $\{x_1, x_2, x_3\}$ *such that* $x_1 > 0$, $x_2 < 0$ *and* $x_3 < 0$.

Proof. Let $y_2 = -x_2$ and $y_3 = -x_3$. Since $-x_1 y_2 - y_2 + x_1 \geq 0$, we have $y_2 < 1$, and similarly $y_3 < 1$. On the other hand, $y_2 y_3 - y_2 - y_3 \geq 0$ implies $y_2 y_3 \geq 4$, a contradiction. ■

Now we may determine the points on E such that the corresponding points (x,y) on Q satisfy (5). Using (3), we obtain that these points are

$$s \in \langle s^{(1)}, s^{(2)} \rangle \cup \langle s^{(3)}, s^{(4)} \rangle,\ t > 0 \quad \text{or} \quad s \in \langle s^{(5)}, s^{(6)} \rangle \cup \langle s^{(7)}, s^{(8)} \rangle,\ t < 0, \tag{6}$$

where

$$\begin{aligned}
s^{(1)} &\approx -79.224984709848, & s^{(2)} &\approx -76.849933010661, \\
s^{(3)} &\approx 458.63743164323, & s^{(4)} &\approx 937.53800125946, \\
s^{(5)} &\approx -82.093984103146, & s^{(6)} &\approx -79.690329099008, \\
s^{(7)} &\approx 232.03689724592, & s^{(8)} &\approx 348.76934786866.
\end{aligned}$$

Our final task is to determine rational points on E which satisfy (6). We know that rational points on E have the form $X = T + mP$, where $T \in \{\mathcal{O}, A, B, C\}$ and $m \in \mathbf{Z}$.

We may parameterize elliptic curve E by Weierstrass function

$$s = \wp(z), \quad t = \frac{1}{2}\wp'(z).$$

The parameter z corresponding to the point $X = (s,t)$, we will denote by $\omega(X)$. Weierstrass $\wp$-function is periodic, with complex and real periods given by

$$\begin{aligned}
\omega_1 &= i \int_{-\infty}^{-84} \frac{ds}{\sqrt{1001700 + 18981s - s^3}} \approx 0.391753653118\, i\,, \\
\omega_2 &= \int_{159}^{+\infty} \frac{ds}{\sqrt{s^3 - 18981s - 1001700}} \approx 0.203439216566
\end{aligned}$$

(see [11, pp. 22-29]). We have $\omega(A) = \frac{\omega_2}{2}$, $\omega(B) = \frac{\omega_2}{2} + \frac{\omega_1}{2}\, i$, $\omega(C) = \frac{\omega_1}{2}\, i$. Using PARI [2], we find that $\omega(P) = \sigma$, where

$$\sigma \approx 0.0218157627564\,.$$

Also using PARI, we find that the condition (6) is equivalent to

$$\omega(X) \in \langle \gamma^{(1)}, \delta^{(1)} \rangle \cup \langle \gamma^{(1)} + \frac{\omega_2}{2}, \delta^{(1)} + \frac{\omega_2}{2} \rangle \tag{7}$$

or

$$\omega(X) - \frac{\omega_1}{2}\, i \in \langle \gamma^{(2)}, \delta^{(2)} \rangle \cup \langle \gamma^{(2)} + \frac{\omega_2}{2}, \delta^{(2)} + \frac{\omega_2}{2} \rangle\,, \tag{8}$$

where

$$\gamma^{(1)} \approx 0.0545490289958\,, \quad \delta^{(1)} \approx 0.0689863420434\,,$$
$$\gamma^{(2)} \approx 0.0525347833467\,, \quad \delta^{(2)} \approx 0.0710005876925\,.$$

Note that points X and $A + X$ induce the same quintuple. Namely, if X induce the point (x, y) on Q, then $A + X$ induce the point $(\frac{6}{x}, \frac{6y}{x^2})$, and the only effect of these changes on R_i's is the permutation of $R_2(x, y)$ and $R_3(x, y)$. Therefore, it suffices to consider the points of the form mP and $C + mP$.

The point $X = mP$ satisfies condition (7) iff

$$m\sigma \bmod \frac{\omega_2}{2} \in \langle \gamma^{(1)}, \delta^{(1)} \rangle$$

or, equivalently,

$$m \cdot (\frac{2\sigma}{\omega_2}) \bmod 1 \in \langle \frac{2\gamma^{(1)}}{\omega_2}, \frac{2\delta^{(1)}}{\omega_2} \rangle\,. \tag{9}$$

Analogously, the point $X = C + mP$ satisfies condition (8) iff

$$m \cdot (\frac{2\sigma}{\omega_2}) \bmod 1 \in \langle \frac{2\gamma^{(2)}}{\omega_2}, \frac{2\delta^{(2)}}{\omega_2} \rangle\,. \tag{10}$$

Assume that $\frac{2\sigma}{\omega_2} = \frac{k}{l} \in \mathbf{Q}$. Then $\omega(2lP) = 0$, which means that P is a torsion point, a contradiction. Therefore $\frac{2\sigma}{\omega_2}$ is an irrational number and we may apply Bohl-Sierpiński-Weyl theorem (see [13, pp. 24-27]), which implies that the sequence $\{m \cdot (\frac{2\sigma}{\omega_2}) \bmod 1\}$ is dense in $[0, 1]$.

Therefore, there are infinitely many integers m which satisfy condition (9), resp. (10), and then the corresponding points mP, $C+mP$ on $E(\mathbf{Q})$ satisfy conditions (7), resp. (8).

Hence, we proved

Theorem 2 *There exist infinitely many Eulerian quintuples consisting of positive rationals.*

Example 1 Condition (9) can be approximated by

$$m \cdot 0.214469590718 \bmod 1 \in \langle 0.536286571189,\ 0.678201019526 \rangle,$$

and condition (10) by

$$m \cdot 0.214469590718 \bmod 1 \in \langle 0.51646663051,\ 0.698002960205 \rangle.$$

It is easy to find "small solutions" of (9):

$$\begin{aligned} m \in M_1 \ = \ & \{\ldots, -100, -95, -86, -81, -72, -67, -58, -53, -44, -39, -30, -25, -16, \\ & -11, -2, 3, 12, 17, 26, 31, 40, 45, 54, 59, 68, 73, 82, 87, 96, \ldots\}, \end{aligned}$$

and of (10):

$$\begin{aligned} m \in M_2 \ = \ & \{\ldots, -100, -95, -90, -86, -81, -72, -67, -58, -53, -44, -39, -30, -25, \\ & -16, -11, -2, 3, 12, 17, 26, 31, 40, 45, 54, 59, 68, 73, 82, 87, 91, 96, \ldots\}. \end{aligned}$$

Note that for $i = 1, 2$ it holds $m \in M_i$ iff $1 - m \in M_i$. Namely, the points mP and $A + (1 - m)P$ induce the same point on Q. This fact explains why $\gamma^{(1)} + \delta^{(1)} = \gamma^{(2)} + \delta^{(2)} = \sigma + \frac{\omega_2}{2}$.

Note also that for "many" elements m of the set M_i, $i = 1, 2$, it holds $m + 28 \in M$. This happens because 28σ is close to $3\omega_2$.

The Eulerian quintuples induced by the points $-2P$ and $C - 2P$ are listed in the following table:

point on E	Eulerian quintuple
$-2P$	$\left\{\frac{122537388240717681609028093312728053 81}{1335628473872653736133733961581468085 6}, \frac{402280625581345978468093983 33}{202737766604925271257562607 2}, \frac{904102036076757756322317387 35}{264016552841465436885252699 8}, \frac{145924966081583314171992018275332758858 9}{133562847387265373613373396158146808 56}, \frac{16463478877068761615}{200378051669604563}\right\}$
$C-2P$	$\left\{\frac{243840048108266478952509085840250160 17}{122601875197165762698924036306247022 0}, \frac{111745345725318807760778453 73}{122557572473080331255380185 2}, \frac{200408761263308135110463918}{200450485329612350005456055}, \frac{287670780013453292618651769213853277 7}{122601875197165762698924036306247022 0}, \frac{13292539885615174 22}{200378051669604563}\right\}$

Remark 1 In the same manner as in the proof of Theorem 2, we can prove that there are infinitely many Eulerian quintuples consisting of negative rationals, and infinitely many Eulerian quintuples consisting of one negative and four positive rationals.

Remark 2 In [9] we asked the following question: For which non-zero rationals q there exist infinitely many rational Diophantine quintuples with the property $D(q)$. It is clear that it suffices to consider square-free integers q. It was known already to Euler that there exist infinitely many rational Diophantine quintuples with the property $D(1)$ (see [4, p. 517]). In [9], we gave an affirmative answer to the above question for $q = -3$, and Theorem 1 solves the case $q = -1$. In our forthcoming paper we will give an affirmative answer to the above question for a large class of rationals q, including 114 integers in the range $-100 \leq q \leq 100$.

References

[1] A. O. L. Atkin & F. Morain. "Finding suitable curves for the elliptic curve method of factorization." *Math. Comp.* **60** (1993):399–405.

[2] C. Batut, D. Bernardi, H. Cohen & M. Olivier. GP/PARI, Université Bordeaux I, 1994.

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

[4] L. E. Dickson. *History of the Theory of Numbers, Vol. 2*, New York: Chelsea, 1966.

[5] Diophantus of Alexandria. *Arithmetics and the Book of Polygonal Numbers*, (I. G. Bashmakova, Ed.), Moscow: Nauka, 1974 (in Russian).

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

[7] A. Dujella. "Complete solution of a family of simultaneous Pellian equations." *Acta Math. Inform. Univ. Ostraviensis* **6** (1998):59–67.

[8] A. Dujella. "An extension of an old problem of Diophantus and Euler." *Fibonacci Quart.* **37** (1999):312–314.

[9] A. Dujella. "A note on Diophantine quintuples." Proceedings of the Conference on Algebraic Number Theory and Diophantine Analysis, Graz, 1998, to appear.

[10] K. S. Kedlaya. "Solving constrained Pell equations." *Math. Comp.* **67** (1998):833–842.

[11] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*, New York: Springer-Verlag, 1993.

[12] S. P. Mohanty & A. M. S. Ramasamy. "The simultaneous Diophantine equations $5y^2 - 20 = x^2$ and $2y^2 + 1 = z^2$." *J. Number Theory* **18** (1984):356–359.

[13] I. Niven. *Diophantine Approximations*, New York: John Wiley, 1963.

[14] SIMATH manual, Universität des Saarlandes, Saarbrücken, 1997.

AMS Classification Numbers: 11G05, 11D09