Irregular Diophantine m-tuples and elliptic curves of high rank

By Andrej Dujella

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

(Communicated by Shigefumi Mori, M. J. A., May 12, 2000)

Abstract: A rational Diophantine m-tuple is a set of m nonzero rationals such that the product of any two of them is one less than a perfect square. In this paper we characterize the notions of regular Diophantine quadruples and quintuples, introduced by Gibbs, by means of elliptic curves. Motivated by these characterizations, we find examples of elliptic curves over $\mathbf{Q}$ with torsion group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and with rank equal 8.

Key words: Elliptic curve; rank; torsion group; Diophantine m-tuple.

1. Diophantine m-tuples. A set of m nonzero rationals $\{a_1, a_2, \dots, a_m\}$ is called a (*rational*) *Diophantine m-tuple* if $a_ia_j + 1$ is a square of a rational number for all $1 \le i < j \le m$ (see [4]). The first example of a Diophantine quadruple was the set $\{1/16, 33/16, 17/4, 105/16\}$ found by Diophantus (see [3]).

Let $\{a, b, c\}$ be a Diophantine triple and let

$$d = a + b + c + 2abc \pm 2\sqrt{(ab+1)(ac+1)(bc+1)}.$$

Arkin, Hoggatt and Strauss [1] proved that $ad + 1$, $bd + 1$ and $cd + 1$ are perfect squares.

Let $\{a, b, c, d\}$ be a Diophantine quadruple such that $abcd \neq 1$ and let

$$\begin{aligned} e = &\frac{1}{(abcd-1)^2}\{(a+b+c+d)(abcd+1) \\ &+2abc + 2abd + 2acd + 2bcd \\ &\pm 2\sqrt{(ab+1)(ac+1)(ad+1)(bc+1)(bd+1)(cd+1)}\}. \end{aligned}$$

In [4] we proved that $ae+1$, $be+1$, $ce+1$ and $de+1$ are perfect squares.

Using the terminology from [6], we will say that a Diophantine quadruple $\{a, b, c, d\}$ is *regular* if it is obtained by the construction from [1]. Equivalently, $\{a, b, c, d\}$ is regular iff a, b, c, d satisfy the relation

$$(1) \qquad (a - b - c + d)^2 = 4(ad + 1)(bc + 1).$$

A Diophantine quintuple $\{a, b, c, d, e\}$ is called *regular* if it is obtained by the construction from [4]. Equivalently,

$$(2) \qquad \begin{aligned} &(abcde + 2abc + a + b + c - d - e)^2 \\ &\quad = 4(ab+1)(ac+1)(bc+1)(de+1). \end{aligned}$$

In order to extend a given Diophantine quadruple $\{a, b, c, d\}$ to a quintuple, one has to solve the system

$$(3) \qquad \begin{aligned} ax + 1 = \square, \quad bx + 1 = \square, \\ cx + 1 = \square, \quad dx + 1 = \square. \end{aligned}$$

It is a natural idea to assign to the system (3) the elliptic curve

$$y^2 = (ax+1)(bx+1)(cx+1)(dx+1).$$

By the substitution

$$t = \frac{y(d-a)(d-b)(d-c)}{(dx+1)^2}, \quad s = \frac{(ax+1)(d-b)(d-c)}{dx+1},$$

we obtain the following elliptic curve

$$(4) \quad E: t^2 = s \cdot [s + (b-a)(d-c)] \cdot [s + (c-a)(d-b)].$$

We have three non-trivial rational 2-torsion points on E:

$$\begin{aligned} &A = (0, 0), \quad B = (-(b-a)(d-c), 0), \\ &C = (-(c-a)(d-b), 0), \end{aligned}$$

and another two obvious rational points:

$$\begin{aligned} &P = ((b-a)(c-a),\ (b-a)(c-a)(d-a)), \\ &Q = \big((ad+1)(bc+1), \\ &\qquad \sqrt{(ab+1)(ac+1)(ad+1)(bc+1)(bd+1)(cd+1)}\big). \end{aligned}$$

Proposition 1. *The Diophantine quadruple* $\{a, b, c, d\}$ *is regular if and only if* $2P = \pm Q$.

Proof. Since the first coordinate of the point $2P$ is equal to

$$\frac{1}{4}(a - b - c + d)^2,$$

the statement follows from formula (1). □

1991 Mathematics Subject Classification. 11G05.

Assume that the Diophantine quadruple $\{a,b,c,d\}$ can be extended to the Diophantine quintuple $\{a,b,c,d,e\}$. Then there is another rational point on E:

$$R=\left(\frac{(de+1)(b-a)(c-a)}{ae+1},\ \frac{(b-a)(c-a)(d-a)}{ae+1}\sqrt{\frac{(be+1)(ce+1)(de+1)}{ae+1}}\right).$$

Proposition 2. *The Diophantine quintuple* $\{a,b,c,d,e\}$ *is regular if and only if* $R\pm P=\pm Q$.

Proof. The straightforward computation shows that the condition that the first coordinate of the point Q is equal to the first coordinate of $R+P$ or $R-P$ is equivalent to relation (2). □

2. Curves with the rank equal 8. Let

$$B(F)=\sup\{\operatorname{rank}E(\mathbf{Q}):E(\mathbf{Q})_{\mathrm{tors}}\simeq F\},$$
$$G(F)=\sup\{\operatorname{rank}E(\mathbf{Q}(t)):E(\mathbf{Q}(t))_{\mathrm{tors}}\simeq F\}.$$

Kihara [8], Kulesz [10] and the author [5] proved independently that $G(\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z})\geq 4$, and recently Kulesz [11] proved that $G(\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z})\geq 5$. In [9] Kihara constructed an infinite family of elliptic curves with the rank ≥ 5 over $\mathbf{Q}$ which have three non-trivial rational 2-torsion points, and in [5] an example was given which shows that $B(\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z})\geq 7$.

Propositions 1 and 2 suggest that if an irregular Diophantine quadruple $\{a,b,c,d\}$ is contained in an irregular quintuple $\{a,b,c,d,e\}$, then we may expect that the rank of E, where E is given by (4), over $\mathbf{Q}$ is ≥ 3.

In [7] Gibbs found 12 examples of Diophantine sextuples. We tried to compute the rank of E, using John Cremona's program MWRANK [2], for quadruples $\{a,b,c,d\}$ which are subsets of Gibbs' examples of Diophantine sextuples. In this way we found 2 curves with the rank equal 8 and 4 curves with the rank equal 7. We listed these examples in the Table I.

Table I

$\{a,b,c,d\}$	rank $E(\mathbf{Q})$
$\left\{\frac{17}{448},\frac{2145}{448},\frac{23460}{7},\frac{2352}{7921}\right\}$	8
$\left\{\frac{32}{91},\frac{60}{91},\frac{1878240}{1324801},\frac{15345900}{12215287}\right\}$	8
$\left\{\frac{35}{192},\frac{155}{27},\frac{1235}{48},\frac{180873}{16}\right\}$	7
$\left\{\frac{609}{3520},\frac{455}{2112},\frac{60137}{960},\frac{11874240}{43080851}\right\}$	7
$\left\{\frac{9}{140},\frac{1225}{12},\frac{347072}{176505},\frac{121275}{6724}\right\}$	7
$\left\{\frac{47}{105},\frac{608}{105},\frac{347072}{176505},\frac{121275}{6724}\right\}$	7

Therefore, we proved the following theorem.

Theorem 1. $B(\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z})\geq 8$.

References

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

[2] Cremona, J. E.: Algorithms for Modular Elliptic Curves. Cambridge Univ. Press, Cambridge-New York (1997).

[3] Diophantus of Alexandria: Arithmetics and the Book of Polygonal Numbers (ed. Bashmakova, I. G.). Nauka, Moscow, pp. 103–104, 232 (1974) (in Russian).

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

[5] Dujella, A.: Diophantine triples and construction of high-rank elliptic curves over $\mathbf{Q}$ with three non-trivial 2-torsion points. Rocky Mountain J. Math. (to appear).

[6] Gibbs, P.: Some rational Diophantine sextuples. math.NT/9902081 (preprint).

[7] Gibbs, P.: A generalised Stern-Brocot tree from regular Diophantine quadruples. math.NT/9903035 (preprint).

[8] Kihara, S.: On the rank of elliptic curves with three rational points of order 2. Proc. Japan Acad., **73A**, 77–78 (1997).

[9] Kihara, S.: On the rank of elliptic curves with three rational points of order 2. II. Proc. Japan Acad., **73A**, 151 (1997).

[10] Kulesz, L.: Courbes elliptiques de rang élevé, possédant un sous-groupe de torsion non trivial sur $\mathbf{Q}$ (preprint).

[11] Kulesz, L.: Courbes elliptiques de rang ≥ 5 sur $\mathbf{Q}(t)$ avec un groupe de torsion isomorphe á $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$. C. R. Acad. Sci. Paris Sér. I Math., **329**(6), 503–506 (1999).