Mordell-Weil groups of elliptic curves induced by Diophantine triples

Andrej Dujella

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

Let E be an elliptic curve over $\mathbb{Q}$.

By Mordell's theorem, the group $E(\mathbb{Q})$ of rationals points on E is a finitely generated abelian group. Hence, it is the product of the torsion group and $r \geq 0$ copies of infinite cyclic group:

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r.$$

By Mazur's theorem, we know that $E(\mathbb{Q})_{\text{tors}}$ is one of the following 15 groups:

$\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$,
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$.

On the other hand, it is not know what values of rank r are possible for elliptic curves over $\mathbb{Q}$. The "folklore" conjecture is that a rank can be arbitrary large, but it seems to be very hard to find examples with large rank. The current record is an example of elliptic curve over $\mathbb{Q}$ with rank ≥ 28, found by Elkies in May 2006.

There is even a stronger conjecture that for any of 15 possible torsion groups T we have $B(T) = \infty$, where

$B(T) = \sup\{\text{rank}\,(E(\mathbb{Q})) \,:\, \text{torsion group of } E \text{ over } \mathbb{Q} \text{ is } T\}$.

Montgomery (1987): Proposed the use of elliptic curves with large torsion group and positive rank in factorization.

It follows from results of Montgomery, Suyama, Atkin & Morain (*Finding suitable curves for the elliptic curve method of factorization*, 1993), that $B(T) \geq 1$ for all torsion groups T.

Womack (2000): $B(T) \geq 2$ for all T

Dujella (2003): $B(T) \geq 3$ for all T

$$B(T) = \sup\{\text{rank}\,(E(\mathbb{Q})) \,:\, E(\mathbb{Q})_{\text{tors}} \simeq T\}.$$

The best known lower bounds for $B(T)$:

T	$B(T) \geq$	Author(s)
0	28	Elkies (06)
$\mathbb{Z}/2\mathbb{Z}$	18	Elkies (06)
$\mathbb{Z}/3\mathbb{Z}$	13	Eroshkin (07)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (06)
$\mathbb{Z}/5\mathbb{Z}$	6	D. & Lecacheux (01)
$\mathbb{Z}/6\mathbb{Z}$	7	D. (01,06)
$\mathbb{Z}/7\mathbb{Z}$	5	D. & Kulesz (01), Elkies (06)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/9\mathbb{Z}$	3	D. (01), MacLeod (04), Eroshkin (06)
$\mathbb{Z}/10\mathbb{Z}$	4	D. (05), Elkies (06)
$\mathbb{Z}/12\mathbb{Z}$	3	D. (01,05,06), Rathbun (03,06)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	14	Elkies (05)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	8	Elkies (05)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (00), D. (00,01,06), Campbell & Goins (03), Rathbun (03,06)

`http://web.math.hr/~duje/tors/tors.html`

Construction of high-rank curves

1. Find a parametric family of elliptic curves over $\mathbb{Q}$ which contains curves with relatively high rank (i.e. an elliptic curve over $\mathbb{Q}(t)$ with large generic rank).

2. Choose in given family best candidates for higher rank. A curve is more likely to have large rank if $\#E(\mathbb{F}_p)$ is relatively large for many primes p.

3. Try to compute the rank (Cremona's program MWRANK - very good for curves with rational points of order 2).

High-rank elliptic curves with some other additional properties:

- congruent numbers: $y^2 = x^3 - n^2x$,
  $r = 6$, Rogers (2000)

- Mordell curves: $y^2 = x^3 + k$,
  $r = 12$, Quer (1987)

- curves with $j = 1728$: $y^2 = x^3 + dx$,
  $r = 14$, Elkies & Watkins (2002)

- taxicab problem: $x^3 + y^3 = m$,
  $r = 11$, Elkies & Rogers (2004)

- Diophantine triples:
  $y^2 = (ax + 1)(bx + 1)(cx + 1)$
  $r = 9$, Dujella (2007)

- Diophantine quadruples:
  $y^2 = (ax + 1)(bx + 1)(cx + 1)(dx + 1)$
  $r = 8$, Dujella & Gibbs (2000)

A set $\{a_1, a_2, \ldots, a_m\}$ 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: $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$

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

Baker and Davenport (1969): Fermat's set cannot be extended to a Diophantine quintuple.

D. (2004): There does not exist a Diophantine sextuple and there are only finitely many Diophantine quintuples.

Let $\{a, b, c\}$ be a (rational) Diophantine triple. Define nonnegative rational numbers r, s, t by

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2.$$

In order to extend this triple to a quadruple, we have to solve the system

$$ax + 1 = \square, \qquad bx + 1 = \square, \qquad cx + 1 = \square.$$

It is natural idea to assign to this system the elliptic curve

$$E: \quad y^2 = (ax + 1)(bx + 1)(cx + 1).$$

Transformation $x \mapsto \frac{x}{abc}$, $y \mapsto \frac{y}{abc}$ leads to

$$E': \quad y^2 \;=\; (x + bc)(x + ac)(x + ab).$$

Three rational points on E' of order 2:

$$T_1 = [-bc, 0], \quad T_2 = [-ac, 0], \quad T_3 = [-ab, 0],$$

and also other obvious rational points

$$P = [0, abc], \quad Q = [1, rst].$$

In general, we may expect that the points P and Q will be two independent points of infinite order, and therefore that $\operatorname{rank} E(\mathbb{Q}) \geq 2$. Thus, assuming various standard conjectures, we may expect that the most of elliptic curves induced by Diophantine triples with the above construction will have the Mordell-Weil group $E(\mathbb{Q})$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^3$.

Question: Which other groups are possible here?

Mazur's theorem: $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $m = 1, 2, 3, 4$.

D. (2001): If a, b, c are positive integers, then the cases $m = 2$ and $m = 4$ are not possible.

For each $1 \leq r \leq 9$, there exists a Diophantine triple $\{a, b, c\}$ such that the elliptic curve $y^2 = (ax+1)(bx+1)(cx+1)$ has the torsion group isomorphic to $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$ and the rank equal to r.

$y^2 = ((k-1)x+1)((k+1)x+1)((16k^3-4k)x+1)$
generic rank = 2

$$s(N) = \sum_{p \leq N,\ p \text{ prime}} \frac{\#E(\mathbb{F}_p) + 1 - p}{\#E(\mathbb{F}_p)} \log(p)$$

$s(523) > 22$ & $s(1979) > 33$ & Selmer rank ≥ 8

$k = 3593/2323$, $\boxed{r = 9}$

$y^2 = ((k-1)x+1)(4kx+1)((16k^3-4k)x+1)$

$k = -2673/491$, $\boxed{r = 9}$

For each $0 \leq r \leq 7$, there exists a Diophantine triple $\{a, b, c\}$ such that the elliptic curve $y^2 = (ax+1)(bx+1)(cx+1)$ has the torsion group isomorphic to $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}$ and the rank equal to r.

Curves with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ have the equation of the form

$$y^2 = x(x+\alpha^2)(x+\beta^2), \quad \alpha, \beta \in \mathbb{Q}.$$

Comparison with $y^2 = x(x+ac-ab)(x+bc-ab)$ lead to conditions $ac - ab = \square$, $bc - ab = \square$. A simple way to fulfill these conditions is to choose a and b such that $ab = -1$. Then $ac - ab = ac + 1 = s^2$ and $bc - ab = bc + 1 = t^2$. It remains to find c such that $\{a, -1/a, c\}$ is a Diophantine triple.

Parametric solution:

$$a = \frac{2T+1}{T-2}, \quad c = \frac{8T}{(2T+1)(T-2)}.$$

$T = 7995/6562$, $\boxed{r = 7}$

For each $1 \leq r \leq 4$, there exists a Diophantine triple $\{a, b, c\}$ such that the elliptic curve $y^2 = (ax+1)(bx+1)(cx+1)$ has the torsion group isomorphic to $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}}$ and the rank equal to r.

General form of curves with the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is

$$y^2 = (x+\alpha^2)(x+\beta^2)\left(x + \frac{\alpha^2\beta^2}{(\alpha-\beta)^2}\right).$$

Comparison gives: $\alpha^2 + 1 = bc + 1 = t^2$, $\beta^2 + 1 = ac + 1 = s^2$, $\alpha^2\beta^2 + (\alpha-\beta)^2 = \square$. We have: $\alpha = \frac{2u}{u^2-1}$, $\beta = \frac{v^2-1}{2v}$, and inserting this in third condition we obtain the equation of the form $F(u, v) = z^2$,

Parametric solution: $u = \frac{v^3+v}{v^2-1}$

$v = 7$, $\boxed{r = 3}$

$u = 34/35$, $v = 8$, $\boxed{r = 4}$

For each $0 \le r \le 3$, there exists a Diophantine triple $\{a, b, c\}$ such that the elliptic curve $y^2 = (ax+1)(bx+1)(cx+1)$ has the torsion group isomorphic to $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}}$ and the rank equal to r.

Every elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is induced by a Diophantine triple (D., Campbell & Goins).

Connell, D. (2000): $\boxed{r = 3}$

$$\left\{\frac{408}{145},\ -\frac{145}{408},\ -\frac{145439}{59160}\right\}.$$

D. (2007): $\boxed{r = 3}$ (4-descent, MAGMA)

$$\left\{\frac{451352}{974415},\ -\frac{974415}{451352},\ -\frac{745765964321}{439804159080}\right\}.$$