High rank elliptic curves induced by Diophantine triples and congruent numbers

Andrej Dujella

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

We describe methods used in construction of elliptic curves with relatively high rank in several interesting families of elliptic curves. E.g.

- curves with prescribed torsion group,
- curves induced by Diophantine triples and quadruples,
- congruent and θ-congruent number curves.

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:

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

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

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

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

T	$B(T) \geq$	Author(s)
0	28	Elkies (06)
$\mathbb{Z}/2\mathbb{Z}$	19	Elkies (09)
$\mathbb{Z}/3\mathbb{Z}$	13	Eroshkin (07,08,09)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (06)
$\mathbb{Z}/5\mathbb{Z}$	8	Dujella & Lecacheux (09), Eroshkin (09)
$\mathbb{Z}/6\mathbb{Z}$	8	Eroshkin (08), Dujella & Eroshkin (08), Elkies (08), Dujella (08)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella & Kulesz (01), Elkies (06), Eroshkin (09), Dujella & Lecacheux (09), Dujella & Eroshkin (09)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (09)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (05,08), Elkies (06)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (08)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (09)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	8	Elkies (05), Eroshkin (08), Dujella & Eroshkin (08)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (00), Dujella (00,01,06,08), Campbell & Goins (03), Rathbun (03,06), Flores, Jones, Rollick & Weigandt (07), Fisher (09)

`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); e.g. by Mestre's polynomial method.

2. Choose in given family best candidates for higher rank. General idea: a curve is more likely to have large rank if $|E(\mathbb{F}_p)|$ is relatively large for many primes p. Precise statement: Birch and Swinnerton-Dyer conjecture. More suitable for computation: Mestre's conditional upper bound (assuming BSD and GRH); Mestre-Nagao sums, e.g.

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

3. Try to compute the rank (Cremona's program MWRANK - very good for curves with rational points of order 2), or at least good lower and upper bounds for the rank.

$$G(T) = \sup\{\operatorname{rank} E(\mathbb{Q}(t)) \,:\, E(\mathbb{Q}(t))_{\text{tors}} \cong T\}.$$

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

T	$B(T) \geq$	Author(s)
0	18	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	11	Elkies (2009)
$\mathbb{Z}/3\mathbb{Z}$	7	Elkies (2007)
$\mathbb{Z}/4\mathbb{Z}$	5	Kihara (2004), Elkies (2007)
$\mathbb{Z}/5\mathbb{Z}$	3	Lecacheux (2001), Eroshkin (2009)
$\mathbb{Z}/6\mathbb{Z}$	3	Lecacheux (2001), Kihara (2006), Eroshkin (2008), Woo (2008)
$\mathbb{Z}/7\mathbb{Z}$	1	Kulesz (1998), Lecacheux (2003), Rabarison (2008), Harrache (2009)
$\mathbb{Z}/8\mathbb{Z}$	1	Kulesz (1998), Lecacheux (2002), Rabarison (2008)
$\mathbb{Z}/9\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/10\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/12\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	7	Elkies (2007)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	3	Lecacheux (2001), Elkies (2007), Eroshkin (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	1	Kulesz (1998), Campbell (1999), Lecacheux (2002), Dujella (2007), Rabarison (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	0	Kubert (1976)

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

Upper bounds for the rank:

If E has a rational point of order 2, i.e. an equation of the form $y^2 = x^3 + ax^2 + bx$, by the method of 2-descent, we have

$$r \leq \omega(b) + \omega(b') - 1,$$

where $b' = a^2 - 4b$ and $\omega(b)$ denotes the number of distinct prime factors of b.

For curves with nontrivial torsion point, we have the *Mazur's bound*. Let E be given with its minimal Weierstrass equation, and let E has a rational point of prime order p. Then it holds

$$r \leq m_p = b + a - m - 1,$$

- b is the number of primes with bad reduction;
- a is the number of primes with additive reduction;
- m is the number of primes q with multiplicative reduction which satisfy that p does not divide the exponent of q in the prime factorization of discriminant Δ and $q \not\equiv 1 \pmod{p}$.

Example (Dujella-Lecacheux): Compute the rank of

$$E\ :\ y^2+y=x^3+x^2-171237101607511786 0x+ 885787957535691389512940164.$$

Solution: We have

$$E(\mathbb{Q})_{\text{tors}}=\{\mathcal{O},[888689186,8116714362487],\\ [-139719349,-33500922231893],\\ [-139719349,33500922231892],\\ [888689186,-8116714362488]\}\cong\mathbb{Z}_5.$$

Let us compute Mazur's bound m_5:

$\Delta=-3^{15}\cdot 5^5\cdot 7^5\cdot 11^5\cdot 19^5\cdot 41^5\cdot 127^5\cdot 1409\cdot 10864429,$

so $b=9$, $a=0$, $m=2$, and $r\leq m_5=6$.

We find the following 6 independent points modulo $E(\mathbb{Q})_{\text{tors}}$:

$$[624069446,7758948474007],[763273511,4842863582287]\\ [680848091,5960986525147],[294497588,20175238652299]\\ [-206499124,35079702960532],[676477901,6080971505482],$$

thus proving that rank(E) = 6 (in 2001 that was the highest know rank for curves with torsion $\mathbb{Z}/5\mathbb{Z}$).

High-rank elliptic curves with some other additional properties:

- Mordell curves ($j = 0$): $y^2 = x^3 + k$,
  $r = 15$, Elkies (2009)

- congruent numbers: $y^2 = x^3 - n^2 x$,
  $r = 7$, Rogers (2004)

- $\pi/3$ and $2\pi/3$-congruent numbers:
  $r = 7$, resp. $r = 6$, Janfada & Salami (2010)

- 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:
  $y^2 = (ax + 1)(bx + 1)(cx + 1)$
  $r = 11$, Aguire, Dujella & Peral (2010)

- Diophantine quadruples:
  $y^2 = (ax + 1)(bx + 1)(cx + 1)(dx + 1)$
  $r = 9$, Dujella (2010)

- $E(\mathbb{Q}(i))_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
  $r = 7$, Dujella & Jukić-Bokun (2010)

- $E(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
  $r = 4$, resp. $r = 5$, Jukić-Bokun (2010)

Diophantine m-tuples

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 $1 \leq i < j \leq m$.

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.

Dujella (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 q,s,t by

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

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

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

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

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

Dujella (2007), Aguire, Dujella & Peral (2010): For each $1 \le r \le 11$, 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.

Dujella (2007): For each $0 \le r \le 7$, 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.

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 $0 \leq r \leq 3$, 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)

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

Congruent and θ-congruent number curves

A positive square-free integer n is called a congruent number if it is the area of a right triangle with rational sides; n is congruent if and only if the congruent number elliptic curve $y^2 = x^3 - n^2 x$ has positive rank.

Fujiwara (1997): θ-congruent number curve:

$$y^2 = x^3 + 2snx - (r^2 - s^2)n^2 x,$$

where $0 < \theta < \pi$, $\cos(\theta) = s/r$ with $0 \leq |s| < r$ and $\gcd(r, s) = 1$. A positive integer n is called a θ-congruent number if there is a triangle with rational sides, with one angle θ and the area equal to $n\sqrt{r^2 - s^2}$.

$\theta = \pi/2$ ($r = 1$, $s = 0$) - ordinary congruent number curve
$\theta = \pi/3$ and $2\pi/3$ ($r = 2$, $s = \pm 1$) - also studied by several authors

Kan (2000): If n is the square-free part of $pq(p+q)(2rq+p(r-s))$, for some positive integers p, q with gcd$(p, q) = 1$, then n is a θ-congruent number (i.e. corresponding elliptic curve has positive rank).

Monsky (1994): The formula for the Selmer rank of congruent number curves (an upper bound for the rank; the same parity as the rank)

Dujella, Janfada & Salami (2009): New examples of rank 6 congruent number curves

Janfada & Salami (2010): $\pi/3$-congruent number curve of rank 7; $2\pi/3$-congruent number curve of rank 6 (current records)