Construction of elliptic curves with high rank

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:

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

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.

$y^2 + xy + y = x^3 - x^2 -$

$2006776241557552658503320820933854275093023031217895650 2x+$

$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$

Independent points of infinite order:

P_1=[−212415009125438107329213746 3,259854492051899599030515511070780628911531]

P_2=[23345098660347017568847545 37,188720041954944691808683165528036279315 31]

P_3=[−16717360540623690638790386 63,25170937726114428780850694724131912604913 1]

P_4=[21391302601391566664929821 37,366395091714397292024214596929412975275 31]

P_5=[15347067644671207238854773 37,854295853460176942890210328627810727995 31]

P_6=[−27310794878756770333415750 63,26252181548433219164128407262390214338753 1]

P_7=[27757262668445716497054585 37,128457554740140602488694876990826403699 31]

P_8=[14943857293271889575418338 17,884866055277334059861164945140492334114 51]

P_9=[18684382286208873585090652 57,592374032144377087127251403930593585891 31]

P_{10}=[20089451088257437748665425 37,476906778801255528821517507815414247115 31]

P_{11}=[23483605409180251696516329 37,174929300062005578573403324764488043635 31]

P_{12}=[−14720840070904811744700086 63,24664345065350371419994744154975979846913 1]

P_{13}=[29241286077080612133632889 37,283502644314888785014883564747673758995 31]

P_{14}=[53749938910660618932939345 37,2861889084272633864511750319164798937315 31]

P_{15}=[17096907682333545233340085 57,718988349746860894661597005292159809216 31]

P_{16}=[24509540113535931440725951 87,44452281735326343570492625506107147365 31]

P_{17}=[29692547092735591674646749 37,327668930753662708013336825431604696875 31]

P_{18}=[27119149349416926013328829 37,20684366127783816986504139815065906135 31]

P_{19}=[20078586077996854528778328 937,27796085411378066046560517256246240300915 31]

P_{20}=[21580824502407347743178106 97,349943734019640268099696622418009012547 31]

P_{21}=[20046454582470590224032249 37,480493297807046455224398669998847546753 1]

P_{22}=[29757494509479962649470913 37,333989898260753223202089344101048578691 31]

P_{23}=[−21024904676862851501473478 63,25957639145987578957167739317168720322753 1]

P_{24}=[31158317991506303490219453 7,168104385229980603540109472915660153473931]

P_{25}=[27739310083418652314437718 17,126321628346499210024141162737692758134 51]

P_{26}=[21565811881437684093634613 87,351250929640229088970041505163751780873 31]

P_{27}=[38663304998724125088156591 37,1211977556559442262930369267150258473225 31]

P_{28}=[22308682897735760237786787 37,285587600305974856633870206007686400285 31]

History of elliptic curves rank records:

rank $\geq$	year	Author(s)
3	1938	Billing
4	1945	Wiman
6	1974	Penney & Pomerance
7	1975	Penney & Pomerance
8	1977	Grunewald & Zimmert
9	1977	Brumer - Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao & Kouya
22	1997	Fermigier
23	1998	Martin & McMillen
24	2000	Martin & McMillen
28	2006	Elkies

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

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)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (06)
$\mathbb{Z}/5\mathbb{Z}$	8	Dujella & Lecacheux (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)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (09)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (05), 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), 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).

2. Choose in given family best candidates for higher rank. Genetal idea: a curve is more likely to have large rank if $|E(\mathbb{F}_p)|$ is relatively large for many primes p (Birch and Swinnerton-Dyer conjecture; Meste-Nagao sums).

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.

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

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 (2008)
$\mathbb{Z}/8\mathbb{Z}$	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`

Mestre's polynomial method (1991):

Lemma: Let $p(x) \in \mathbb{Q}[x]$ be a monic polynomial and $\deg p = 2n$. Then there exist unique polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that $p = q^2 - r$ and $\deg r \leq n - 1$.

The polynomial q can be obtained from the asymptotic expansion of $\sqrt{p}$.

Assume now that $p(x) = \prod_{i=1}^{2n}(x - a_i)$, where $a_1, \dots, a_{2n}$ are distinct rationals. The curve

$$C : \quad y^2 = r(x)$$

contains the points $(a_i, \pm q(a_i))$, $i = 1, \dots, 2n$. If $\deg r = 3$ or 4, and $r(x)$ has only simple roots, then C is an elliptic curve. This statement is clear for $\deg r = 3$. If $\deg r = 4$, we choose one rational point on C (e.g. $(a_1, q(a_1))$) for the points in infinity and transform C into an elliptic curve.

For $n = 5$, almost all choices of a_i's give $\deg r = 4$. Then C has 10 rational points of the form $(a_i, q(a_i))$ and by the mentioned transformation we may expect to obtain an elliptic curve with rank ≥ 9. Mestre constructed a family of elliptic curves (i.e. a curve over $\mathbb{Q}(t)$) with rank ≥ 11, by taking $n = 6$ and $a_i = b_i + t$, $i = 1, \dots, 6$; $a_i = b_{i-6} - t$, $i = 7, \dots, 12$, and by choosing numbers $b_1, \dots, b_6$ in such a way that the coefficient with x^5 in $r(x)$ be equal to 0 (e.g. $b_1 = -17$, $b_2 = -16$, $b_3 = 10$, $b_4 = 11$, $b_5 = 14$, $b_6 = 17$).

- extended by Mestre, Nagao and Kihara up to rank 14 over $\mathbb{Q}(t)$

- generalized by Fermigier, Kulesz and Lecacheux to curves with nontrivial torsion group

- Elkies (2006): rank 18 over $\mathbb{Q}(t)$ (methods from algebraic geometry)

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

$$E\,:\; y^2+y=x^3+x^2-1712371016075117860x+ \\ 8857879575356913895129 40164.$$

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 $r\le m_5=6$.

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

$$[624069446,7758948474007],[763273511,4842863582287] \\ [680848091,5960986525147],[294497588,20175238652299] \\ [-206499124,3507970296 0532],[676477901,6080971505482],$$

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)

- 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)

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

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.

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 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

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

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

Meste-Nagao sum:

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

$s(523) > 22$ & $s(1979) > 33$ & 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 $0 \le r \le 7$, 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.

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 $0 \leq r \leq 3$, 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)

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