Construction of high rank elliptic curves and related Diophantine problems

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.

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

$2006776241557552658503320820933854275093023031217895650 2x +$

$34481611795030556467032985690390720374855944359319180361266008296291939448732243429$

Independent points of infinite order:

P_1=[−212415009125438107329213746 3,259854492051899599030515511070780628911531]

P_2=[233450986603470175688475453 7,188720041954944691808683165528036279315 31]

P_3=[−167173605406236906387903866 3,251709377261144287808506947241319126049131]

P_4=[213913026013915666649298213 7,366395091714397292024214596929412975275 31]

P_5=[153470676446712072388547733 7,854295853460176942890210328627810727995 31]

P_6=[−273107948787567703334157506 3,262521815484332191641284072623902143387531]

P_7=[277572626684457164970545853 7,128457554740140602488694876990826403699 31]

P_8=[149438572932718895754183381 7,884866055277334059861164945140492334114 51]

P_9=[186843822862088735850906525 7,592374032144377087127251403930593585891 31]

P_{10}=[200894510882574377486654253 7,476906778801255528821517507815414247115 31]

P_{11}=[234836054091802516965163293 7,174929300062005578573403324764488043635 31]

P_{12}=[−147208400709048117447000866 3,246643450653503714199947441549759798469131]

P_{13}=[292412860770806121336328893 7,283502644314888785014883564747673758995 31]

P_{14}=[537499389106606189329393453 7,286188908427263386451175031916479893731531]

P_{15}=[170969076823335452333400855 7,718988349746860894661597005292159809216 31]

P_{16}=[245095401135359314407259518 7,444522817353263435704926255061071473653 1]

P_{17}=[296925470927355916746467493 7,327668930753662708013336825431604696875 31]

P_{18}=[271191493494169260133288293 7,206843661277838169865041398150659061353 1]

P_{19}=[200785860779968545287783289 37,277960854113780660465605172562462403009 1531]

P_{20}=[215808245024073477431781069 7,349943734019640268099696622418009012547 31]

P_{21}=[200464545824705902240322493 7,480493297807046455224398669998884754675 31]

P_{22}=[297574945094799626494709133 7,333989898260753223202089344101048578691 31]

P_{23}=[−210249046768628515014734786 3,259576391459875789571677393171687203227531]

P_{24}=[311583179915063034902194537,168104385229980603540109472915660153473931]

P_{25}=[277393100834186523144377181 7,126321628346499210024141162737692758134 51]

P_{26}=[215658118814376840936346138 7,351250929640229088970041505163751780873 31]

P_{27}=[386633049987241250881565913 7,121197755655944226293036926715025847322531]

P_{28}=[223086828977357602377867873 7,285587600305974856633870206007686400285 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`

The problem of the construction of high-rank elliptic curves has some relevance for cryptography. Namely, the discrete logarithm problem for multiplicative group $\mathbb{F}_q^*$ of a finite field can be solved in subexponential time using the Index Calculus method. For this reason, it was proposed by Miller and Koblitz in 1985 that for cryptographic purposes, one should replace F_q^* by the group of rational points $E(\mathbb{F}_q)$ on an elliptic curve over finite field.

DLP in $\mathbb{F}_p^*$:
$\mathbb{F}_p^* \to \mathbb{Z}$; factor base $\mathcal{F}$ = small primes

ECDLP: $E(\mathbb{F}_p) \to E(\mathbb{Q})$;
factor base $\mathcal{F}$ = generators of $E(\mathbb{Q})$

The main reasons why Index Calculus method cannot be applied on elliptic curves are that it is difficult:

- to find elliptic curves with large rank,

- to find elliptic curves generated by points of small height,

- to lift a point of $E(\mathbb{F}_p)$ to a point of $E(\mathbb{Q})$.

Silverman & Suzuki (1998):
For $p \approx 2^{160}$, we need $r \approx 180$.

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), Eroshkin (07)
$\mathbb{Z}/7\mathbb{Z}$	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), Eroshkin & Dujella (07)
$\mathbb{Z}/10\mathbb{Z}$	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), Flores, Jones, Rollick & Weigandt (07)

`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).

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

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

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

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

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)
  (published in Proc. Japan Acad.)

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: $E(\mathbb{Q})_{\mathsf{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ 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 $0 \leq r \leq 3$, 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)

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

Let us consider arithmetic progressions consisting of integers which are y-components of solutions of a Pellian equation of the form

$$x^2 - dy^2 = m.$$

A. Pethő and V. Ziegler (to appear in JNT):

- for the four-term arithmetic progression $1, 3, 5, 7$ there exists Pellian equation $x^2 - dy^2 = m$, where d is not a square, such that $1, 3, 5, 7$ are y-components of the solutions of this equation.

- for the arithmetic progressions $0, 1, 2, 3$ such an equation does not exist.

- for a five-terms arithmetic progression $y_1 < y_2 < y_3 < y_4 < y_5$ (such that $|y_i| \neq |y_j|$ for any $i \neq j$) there are at most finitely many $d, m \in \mathbb{Z}$ such that d is not a square, $m \neq 0$ and $\gcd(d, m)$ is square-free such that y_1, y_2, y_3, y_4, y_5 are the y-components of solutions to $x^2 - dy^2 = m$.

D. & A. Pethő & P. Tadić (to appear in Acta Math. Hungar.):

- apart from $0, 1, 2, 3$ and $-3, -2, -1, 0$, for all four-term arithmetic progression consisting of integers there exist infinitely many equations of the form $x^2 - dy^2 = m$, where d is not a square (if d is a square and $m = 0$, the problem is trivial) and $\gcd(d, m)$ is square-free (so that the equations are essentially distinct) for which the elements of the given progression form y-components of solutions.

- there exist arithmetic progressions with five, six and seven elements which are y-components of solutions of a Pellian equation.

The system

$$\begin{aligned} X_1^2 - da^2 &= m, \\ X_2^2 - d(a+k)^2 &= m, \\ X_3^2 - d(a+2k)^2 &= m, \\ X_4^2 - d(a+3k)^2 &= m \end{aligned}$$

of Diophantine equations defines the curve of genus 1.

It can be transformed ($T = a/k$) to the elliptic curve $\mathcal{E}$:

$$\begin{aligned} y^2 = {} & x^3 + (176T^2 + 672T + 628)x^2 + (9216T^4 + 72192T^3 + 209664T^2 \\ & + 267648T + 126720)x + 147456T^6 + 1769472T^5 + 8773632T^4 \\ & + 23003136T^3 + 33629184T^2 + 25989120T + 8294400. \end{aligned}$$

Shioda's formula $\Rightarrow \operatorname{rang}_{\mathbb{Q}(T)}\mathcal{E} = 1$.

generator:

$P := [-64T^2 - 256T - 240, 128T^3 + 640T^2 + 992T + 480]$

e.g. rang $= 7$ for $T = 619/6089$

For $(a, k) = (-461, 166)$ we obtain the elliptic curve

$$y^2 = x^3 + 3283392x^2 + 1816362270720x + 233361525187805184$$

of rank 2, with generators

$$P_1 = [2025472, 5068743680],$$

$$P_2 = [-183168, 68382720].$$

The point P_2 gives the equation

$$x^2 + 1245y^2 = 375701326$$

with the property that the seven numbers $a, a+k, a+2k, a+3k, a+4k, a+5k, a+6k$, i.e.

$$y = -461, -295, -129, 37, 203, 369, 535$$

are solutions of this equation.

This is the longest known arithmetic progression (with distinct absolute values) on curves of the form $x^2 - dy^2 = m$.