High rank elliptic curves with prescribed torsion group

Andrej Dujella

University of Zagreb

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.

$$y^2+xy+y=x^3-x^2-20067762415575526585033208209338542750930230312178956502x+3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

Independent points of infinite order:

P_1=[−2124150091254381073292137463,259854492051899599030515511070780628911531]

P_2=[2334509866034701756884754537,188720041954944691808683165528036279315 31]

P_3=[−1671736054062369063879038663,251709377261144287808506947241319126049131]

P_4=[2139130260139156666492982137,366395091714397292024214596929412975275 31]

P_5=[1534706764467120723885477337,854295853460176942890210328627810727995 31]

P_6=[−2731079487875677033341575063,262521815484332191641284072623902143387531]

P_7=[2775726266844571649705458537,128457554740140602488694876990826403699 31]

P_8=[1494385729327188957541833817,884866055277334059861164945140492334114 51]

P_9=[1868438228620887358509065257,592374032144377087127251403930593585891 31]

P_{10}=[2008945108825743774866542537,476906778801255528821517507815414247115 31]

P_{11}=[2348360540918025169651632937,174929300062005578573403324764488043635 31]

P_{12}=[−1472084007090481174470008663,246643450653503714199947441549759798469131]

P_{13}=[2924128607708061213363288937,283502644314888785014883564747673758995 31]

P_{14}=[5374993891066061893293934537,2861889084272633864511750319164798937315 31]

P_{15}=[1709690768233354523334008557,718988349746860894661597005292159809216 31]

P_{16}=[2450954011353593144072595187,44452281735326343570492625506107147365 31]

P_{17}=[2969254709273559167464674937,327668930753662708013336825431604696875 31]

P_{18}=[2711914934941692601332882937,20684366127783816986504139815065906135 31]

P_{19}=[2007858607799685452877832893 7,2779608541137806604656051725624624030091531]

P_{20}=[2158082450240734774317810697,349943734019640268099696622418009012547 31]

P_{21}=[2004645458247059022403224937,480493297807046455224398669998884754675 31]

P_{22}=[2975749450947996264947091337,333989898260753223202089344101048578691 31]

P_{23}=[−2102490467686285150147347863,25957639145987578957167739317168720322 7531]

P_{24}=[3115831799150630349021945 37,168104385229980603540109472915660153473931]

P_{25}=[2773931008341865231443771817,126321628346499210024141162737692758134 51]

P_{26}=[2156581188143768409363461387,351250929640229088970041505163751780873 31]

P_{27}=[3866330499872412508815659137,1211977556559442262930369267150258473225 31]

P_{28}=[2230868289773576023778678737,285587600305974856633870206007686400285 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: $E(\mathbb{F}_q) \to E(\mathbb{Q})$;
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

$B(T) = \sup\{\text{rank}\,(E(\mathbb{Q}))$: torsion group of E over $\mathbb{Q}$ 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)
$\mathbb{Z}/3\mathbb{Z}$	12	Eroshkin (06)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (06)
$\mathbb{Z}/5\mathbb{Z}$	6	Dujella & Lecacheux (01)
$\mathbb{Z}/6\mathbb{Z}$	7	Dujella (01,06)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella & Kulesz (01)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/9\mathbb{Z}$	3	Dujella (01), MacLeod (04)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (05), Elkies (06)
$\mathbb{Z}/12\mathbb{Z}$	3	Dujella (01,05,06), Rathbun (2003)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	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), Dujella (00,01,06), Campbell & Goins (03), Rathbun (03)

`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).

The similar methods can be applied in construction of high-rank elliptic curves with some other additional properties:

- congruent numbers: $y^2 = x^3 - n^2 x$,
  $r = 6$, 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 (2006)

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

family
$y^2 = ((k-1)x+1)((k+1)x+1)((16k^3-4k)x+1)$
has generic rank equal to 2
(points with infinite order with x-coordinates 0 and $1/((k-1)(k+1)(16k^3-4k)))$

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

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

$k = 3593/2323$, $r = 9$