Elliptic curves with large rank

Andrej Dujella

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

Elliptic curves

Let $\mathbb{K}$ be a field. An *elliptic curve* over $\mathbb{K}$ is a nonsingular projective cubic curve over $\mathbb{K}$ with at least one $\mathbb{K}$-rational point. Each such curve can be transformed by birational transformations to the equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (1)$$

which is called the *Weierstrass form*.

If char($\mathbb{K}$) $\neq 2, 3$, then the equation (1) can be transformed to the form

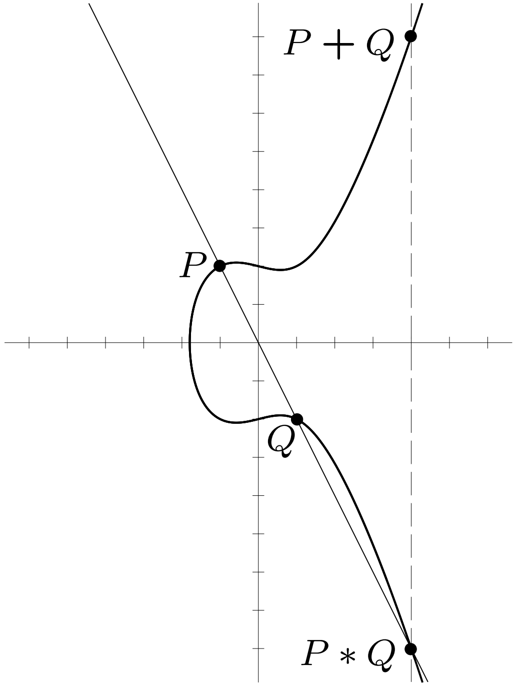
$$y^2 = x^3 + ax + b, \tag{2}$$

which is called the *short Weierstrass form*. Now the nonsingularity means that the cubic polynomial $f(x) = x^3 + ax + b$ has no multiple roots (in algebraic closure $\overline{\mathbb{K}}$), or equivalently that the *discriminant* $\Delta = -4a^3 - 27b^2$ is nonzero.

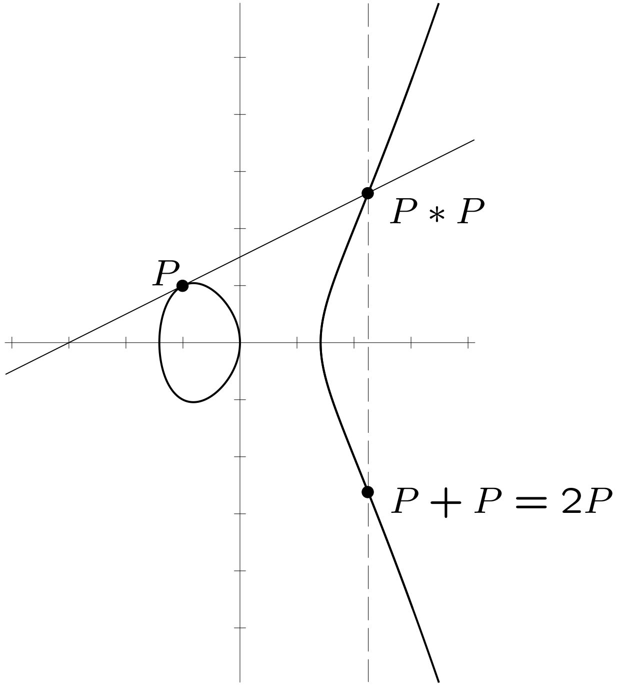
One of the most important facts about elliptic curves is that the set $E(\mathbb{K})$ of $\mathbb{K}$-rational points on an elliptic curve over $\mathbb{K}$ (affine points (x, y) satisfying (1) along with the point at infinity) forms an abelian group in a natural way.

In order to visualize the group operation, assume for the moment that $\mathbb{K} = \mathbb{R}$ and consider the set $E(\mathbb{R})$. Then we have an ordinary curve in the plane. It has one or two components, depending on the number of real roots of the cubic polynomial $f(x) = x^3 + ax + b$.

Let E be an elliptic curve over $\mathbb{R}$, and let P and Q be two points on E. We define $-P$ as the point with the same x-coordinate but negative y-coordinate of P. If P and Q have different x-coordinates, then the straight line though P and Q intersects the curve in exactly one more point, denoted by $P * Q$. We define $P + Q$ as $-(P * Q)$. If $P = Q$, then we replace the secant line by the tangent line at the point P. We also define $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P \in E(\mathbb{R})$, where $\mathcal{O}$ is the point in infinity.



secant line



tangent line

Torsion and rank of elliptic curves over $\mathbb{Q}$

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

By the Mordell-Weil 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 the 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 known which 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.

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

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

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

T	$B(T) \geq$	Author(s)
0	28	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	19	Elkies (2009)
$\mathbb{Z}/3\mathbb{Z}$	13	Eroshkin (2007,2008,2009)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (2006)
$\mathbb{Z}/5\mathbb{Z}$	8	Dujella & Lecacheux (2009), Eroshkin (2009)
$\mathbb{Z}/6\mathbb{Z}$	8	Eroshkin (2008), Dujella & Eroshkin (2008), Elkies (2008), Dujella (2008), Dujella & Peral (2012)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella & Kulesz (2001), Elkies (2006), Eroshkin (2009), Dujella & Lecacheux (2009), Dujella & Eroshkin (2009)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (2009)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005,2008), Elkies (2006)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (2009)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	9	Dujella & Peral (2012)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (2000), Dujella (2000,2001,2006,2008), Campbell & Goins (2003), Rathbun (2003,2006), Flores, Jones, Rollick & Weigandt (2007), Fisher (2009)

Construction of high-rank curves

1. Find a parametric family of elliptic curves over $\mathbb{Q}$ that 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 or by using elliptic curves induced by Diophantine triples.

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. the sum:

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

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.

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

T	$G(T) \geq$	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), Dujella & Peral (2012)
$\mathbb{Z}/7\mathbb{Z}$	1	Kulesz (1998), Lecacheux (2003), Rabarison (2008), Harrache (2009)
$\mathbb{Z}/8\mathbb{Z}$	2	Dujella & Peral (2012)
$\mathbb{Z}/9\mathbb{Z}$	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)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	4	Dujella & Peral (2012)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	2	Dujella & Peral (2012)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	0	Kubert (1976)

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), Watkins (2011,2012)

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

- Diophantine triples:
  $y^2 = (ax + 1)(bx + 1)(cx + 1)$
  $r = 11$, Aguirre, Dujella & Peral (2012)

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

- $E(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
  $r = 7$, resp. $r = 6$, Jukić Bokun (2011)

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

Diophantus of Alexandria: $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$

Fermat: $\{1, 3, 8, 120\}$ (Euler: $777480/2879^2$)

Baker & 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. 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

$$E:\qquad y^2=(ax+1)(bx+1)(cx+1),$$

and we will say that elliptic curve E is *induced by the Diophantine triple* $\{a,b,c\}$.

Dujella & Peral (2012):

Elliptic curves with the torsion subgroup $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}$

Such curves have an equation of the form

$$y^2 = x(x + x_1^2)(x + x_2^2), \qquad x_1, x_2 \in \mathbb{Q}.$$

The point $[x_1 x_2, x_1 x_2(x_1 + x_2)]$ is a rational point on the curve of order 4.

The coordinate transformation $x \mapsto \frac{x}{abc}$, $y \mapsto \frac{y}{abc}$ applied to the curve E leads to $y^2 = (x + ab)(x + ac)(x + bc)$, and by translation we obtain the equation

$$y^2 = x(x + ac - ab)(x + bc - ab).$$

If we can find a Diophantine triple a, b, c such that $ac - ab$ and $bc - ab$ are perfect squares, then the elliptic curve induced by $\{a, b, c\}$ will have the torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. We may expect that this curve will have positive rank, since it also contains the point $[ab, abc]$.

A convenient 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 a and c such that $\{a, -1/a, c\}$ is a Diophantine triple. A parametric solution is

$$a = \frac{\alpha\tau + 1}{\tau - \alpha}, \quad c = \frac{4\alpha\tau}{(\alpha\tau + 1)(\tau - \alpha)}.$$

After some simplifications, we get

$$y^2 = x^3 + 2(\alpha^2 + \tau^2 + 4\alpha^2\tau^2 + \alpha^4\tau^2 + \alpha^2\tau^4)x^2$$
$$+ (\tau + \alpha)^2(\alpha\tau - 1)^2(\tau - \alpha)^2(\alpha\tau + 1)^2 x.$$

To increase the rank, we now force the points with x-coordinates

$$(\tau+\alpha)^2(\alpha\tau-1)(\alpha\tau+1) \quad \text{and} \quad (\tau+\alpha)(\alpha\tau-1)^2(\tau-\alpha)$$

to lie on the elliptic curve. We get the conditions

$$\tau^2 + \alpha^2 + 2 = \square \quad \text{and} \quad \alpha^2\tau^2 + 2\alpha^2 + 1 = \square,$$

with a parametric solution

$$\tau = \frac{(3t^2 + 6t + 1)(5t^2 + 2t - 1)}{4t(t-1)(3t+1)(t+1)},$$
$$\alpha = -\frac{(t+1)(7t^2 + 2t + 1)}{t(t^2 + 6t + 3)}.$$

We get the elliptic curve

$$y^2 = x^3 + A(t)x^2 + B(t)x,$$

where

$$\begin{aligned}A(t) = 2(&87671889t^{24} + 854321688t^{23} + 3766024692t^{22} + 9923033928t^{21}\\ &+ 17428851514t^{20} + 21621621928t^{19} + 19950275060t^{18}\\ &+ 15200715960t^{17} + 11789354375t^{16} + 10470452464t^{15} + 8925222696t^{14}\\ &+ 5984900048t^{13} + 2829340620t^{12} + 820299856t^{11} + 59930952t^{10}\\ &- 66320528t^{9} - 35768977t^{8} - 9381000t^{7} - 1017244t^{6} + 262760t^{5}\\ &+ 159130t^{4} + 41096t^{3} + 6468t^{2} + 600t + 25),\\ B(t) = (&t^2 - 2t - 1)^2(69t^4 + 148t^3 + 78t^2 + 4t + 1)^2(13t^2 - 2t - 1)^2\\ &\times (9t^4 + 28t^3 + 18t^2 + 4t + 1)^2(11t^4 + 12t^3 + 2t^2 - 4t - 1)^2\\ &\times (9t^2 + 14t + 7)^2(31t^4 + 52t^3 + 22t^2 - 4t - 1)^2(3t^2 + 2t + 1)^2,\end{aligned}$$

with rank ≥ 4 over $\mathbb{Q}(t)$. Indeed, it contains the points whose x-coordinates are

$$
\begin{aligned}
X_1 &= (9t^4+28t^3+18t^2+4t+1)^2(11t^4+12t^3+2t^2-4t-1)^2 \\
&\quad\times(69t^4+148t^3+78t^2+4t+1)^2, \\
X_2 &= (3t^2+2t+1)(9t^2+14t+7)^2(13t^2-2t-1) \\
&\quad\times(9t^4+28t^3+18t^2+4t+1)(11t^4+12t^3+2t^2-4t-1)^2 \\
&\quad\times(31t^4+52t^3+22t^2-4t-1), \\
X_3 &= (3t^2+2t+1)(9t^2+14t+7)^2(13t^2-2t-1) \\
&\quad\times(9t^4+28t^3+18t^2+4t+1)^2(11t^4+12t^3+2t^2-4t-1) \\
&\quad\times(69t^4+148t^3+78t^2+4t+1), \\
X_4 &= -(3t^2+2t+1)^2(9t^2+14t+7)^2(11t^4+12t^3+2t^2-4t-1)^2 \\
&\quad\times(31t^4+52t^3+22t^2-4t-1)^2.
\end{aligned}
$$

and a specialization, e.g. $t = 2$, shows that the four points P_1, P_2, P_3, P_4, having these x-coordinates, are independent points of infinite order.

Moreover, since our curve has full 2-torsion, by applying the recent algorithm by Gusić and Tadić we can show that rank$(E(\mathbb{Q}(t))) = 4$ and that the four points P_1, P_2, P_3, P_4 are free generators of $E(\mathbb{Q}(t))$.

Elliptic curves over quadratic fields

Kenku & Momose (1988), **Kamienny (1992)**:
Let E be an elliptic curve over a quadratic field $\mathbb{K}$. The torsion group of $E(\mathbb{K})$ is isomorphic to one of the following groups:
$\mathbb{Z}/n\mathbb{Z}$, where $n = 1, 2, 3, \ldots 16$ or 18;
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, where $n = 1, 2, 3, 4, 5, 6$;
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}$, where $n = 1$ or 2 (only if $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$);
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (only if $\mathbb{K} = \mathbb{Q}(i)$).

Note that if torsion group over a number field $\mathbb{K}$ contains $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, then the m-th roots of unity lie in $\mathbb{K}$.

Najman (2010,2011):

a) The torsion group of an elliptic curve over $\mathbb{Q}(i)$ is isomorphic either to one of the groups from Mazur's theorem or to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

b) The torsion of an elliptic curve over $\mathbb{Q}(\sqrt{-3})$ is isomorphic either to one of the groups from Mazur's theorem, or to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Bosman, Bruin, Dujella, Najman (2012):
There exist elliptic curves over quadratic fields with positive rank and torsion $\mathbb{Z}/15\mathbb{Z}$ (rank ≥ 1 over $\mathbb{Q}(\sqrt{345})$, $\mathbb{Z}/18\mathbb{Z}$ (rank ≥ 2 over $\mathbb{Q}(\sqrt{26521})$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ (rank ≥ 4 over $\mathbb{Q}(\sqrt{55325286553})$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ (rank ≥ 4 over $\mathbb{Q}(\sqrt{2947271015})$).

Together with Rabarison (2010), this implies that there exist curves with positive rank for all 26 possible torsion groups over quadratic fields.

All elliptic curves over quadratic fields with torsions $\mathbb{Z}/13\mathbb{Z}$ or $\mathbb{Z}/18\mathbb{Z}$ have even rank (*false complex multiplication*).

Similar results for cubic and quartic fields.

Aguirre, Dujella, Jukić Bokun, Peral (2012):
For each of 26 possible torsion group, except maybe for $\mathbb{Z}/15\mathbb{Z}$, there exist an elliptic curve over some quadratic field with this torsion group and with rank ≥ 2.

In the case of the 15 possible torsion groups of elliptic curves over $\mathbb{Q}$ (and other torsion groups which admit a model with rational coefficients), we consider curves with rational coefficients, and in order to determine their rank over a quadratic field $\mathbb{Q}(\sqrt{d})$ we use the formula

$$\text{rank}(E(\mathbb{Q}(\sqrt{d})) = \text{rank}(E(\mathbb{Q})) + \text{rank}(E^{(d)}(\mathbb{Q})), \quad (3)$$

where $E^{(d)}$ denotes the d-quadratic twist of E.

We may start with one of the record curves with this torsion over $\mathbb{Q}$, then search for a twist of this curve with high rank, and finally use (3). However, the record curves usually have very large coefficients, which makes it hard to compute the rank of its twist. Thus sometimes it is more profitable to start with curves of rank slightly smaller than the corresponding record, and then use the full power of standard sieving methods for finding high rank curves in parametric families of elliptic curves.

These methods include computations of Mestre-Nagao sums and the Selmer rank. In some cases the root number is used either for reaching conditional results through the Parity Conjecture or as an additional sieving parameter. Our implementations use `Pari/GP` and `mwrank`.

For some torsion groups of odd order (trivial, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$) the largest known ranks were obtained by applying Mestre's result, who proved that for any elliptic curve E over $\mathbb{Q}$ there exist infinitely many quadratic twists with rank ≥ 2, to the record curves over $\mathbb{Q}$.

For the torsion groups of the form $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$, we may take the record curve with torsion $\mathbb{Z}/2m\mathbb{Z}$ over $\mathbb{Q}$, and then determine the quadratic field over which this curve contains torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$.

For the remaining torsion groups, we use the parametrizations given in Rabarison's PhD thesis, and try to compute the rank (or at least to get some information on it) for curves corresponding to small parameters by using procedures available in `Magma`.

T	d	lower bound	Author(s)
0	$*$	30	Elkies
$\mathbb{Z}/2\mathbb{Z}$	-1	28	Watkins
$\mathbb{Z}/3\mathbb{Z}$	$*$	15	Eroshkin
$\mathbb{Z}/4\mathbb{Z}$	-25689	15	ADJBP
$\mathbb{Z}/5\mathbb{Z}$	$*$	10	Dujella & Lecacheux, Eroshkin
$\mathbb{Z}/6\mathbb{Z}$	3521	11	ADJBP
$\mathbb{Z}/7\mathbb{Z}$	$*$	7	Dujella & Kulesz, ...
$\mathbb{Z}/8\mathbb{Z}$	-227	9	ADJBP
$\mathbb{Z}/9\mathbb{Z}$	-155	6	ADJBP
$\mathbb{Z}/10\mathbb{Z}$	-2495	7	ADJBP
$\mathbb{Z}/11\mathbb{Z}$	-3239	2	ADJBP
$\mathbb{Z}/12\mathbb{Z}$	2014	7	ADJBP
$\mathbb{Z}/13\mathbb{Z}$	193	2	Rabarison
$\mathbb{Z}/14\mathbb{Z}$	265	2	Rabarison, ADJBP
$\mathbb{Z}/15\mathbb{Z}$	-7	1	BBDN, ADJBP
$\mathbb{Z}/16\mathbb{Z}$	1785	2	ADJBP
$\mathbb{Z}/18\mathbb{Z}$	26521	2	BBDN
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$*$	19 (20)	Elkies
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	-83201	13	ADJBP
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	624341	10	ADJBP
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	31230597	8	ADJBP
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$	1065333545	4 (5)	BBDN, ADJBP
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	2947271015	4	BBDN
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	-3	7	Jukić Bokun
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	-3	6	Jukić Bokun
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	-1	7	Dujella & Jukić Bokun

Mazur & Rubin (2010): For every number field $\mathbb{K}$ there exist an elliptic curve over $\mathbb{K}$ with rank 0.

Is the same statement valid if we fix torsion group? **Bosman, Bruin, Dujella, Najman (2012): No.**

All elliptic curves over quartic field $\mathbb{Q}(i, \sqrt{5})$ with torsion group $\mathbb{Z}/15\mathbb{Z}$ have positive rank.

Actually, all such curves are isomorphic to the curve $E : y^2 = x^3 + (281880\sqrt{5} - 630315)x - 328392630 + 146861640\sqrt{5}$, which has a point of infinite order $(675 - 300\sqrt{5}, 2052\sqrt{5} - 4590)$ and a point $(584 - 264\sqrt{5}, 5076\sqrt{-5} - 11340i)$ of order 15.

Applications of elliptic curves in factorization

Finding elliptic curves with positive rank and large torsion over number fields is not just a curiosity. Elliptic curves with large torsion and positive rank over the rationals have long been used for factorization, starting with Montgomery, Atkin and Morain. We will try to show that examining the torsion of an elliptic curve over number fields of small degree has some additional benefits.

It is well-known that elliptic curves have applications in cryptography and also in factorization of large integers and primality proving.

The main idea is to replace the group $\mathbb{F}_p^*$ with (fixed) order $p-1$, by a group $E(\mathbb{F}_p)$ with more flexible order. Namely, by the Hasse theorem, we have

$$p+1-2\sqrt{p} < |E(\mathbb{F}_p)| < p+1+2\sqrt{p}.$$

Pollard's $p-1$ factorization method (1974):

Let n be a composite integer with unknown prime factor p. For any multiple m of $p-1$ we have $a^m \equiv 1 \pmod{p}$, and thus $p|\,\mathrm{gcd}(a^m-1, n)$. If $p-1$ is smooth (divisible only by small primes), then we can guess a multiple of $p-1$ by taking $m = \mathrm{lcm}(1, 2, ..., B)$ for a suitable number B.

In 1985, Lestra proposed the Elliptic curve factorization method (ECM), in which the group $\mathbb{F}_p^*$ is replaced by a group $E(\mathbb{F}_p)$, for a suitable chosen elliptic curve E. In ECM, one hopes that the chosen elliptic curve will have smooth order over a prime field. It is now a classical method to use for that purpose elliptic curves E with large rational torsion over $\mathbb{Q}$ (and known point of infinite order), as the torsion will inject into $E(\mathbb{F}_p)$ for all primes p of good reduction. This in turn makes the order of $E(\mathbb{F}_p)$ more likely to be smooth.

We say that an integer m is n-*smooth*, for some fixed value n if all the prime divisors of m are less or equal than n. Choosing elliptic curves E for the elliptic curve factoring method, one wants to choose elliptic curves such that the order $E(\mathbb{F}_p)$ is smooth. Standard heuristics say that larger torsion of $E(\mathbb{Q})$ implies a greater probability that $|E(\mathbb{F}_p)|$ is smooth. This is because the torsion of $E(\mathbb{Q})$ will inject into $E(\mathbb{F}_p)$ for all primes p of good reduction, making $|E(\mathbb{F}_p)|$ divisible by the order of the torsion of $E(\mathbb{Q})$.

But this is not necessary so straightforward, as a curve with smaller $E(\mathbb{Q})_{\text{tors}}$ can have much larger torsion over fields of small degree, giving all together a greater probability of $|E(\mathbb{F}_p)|$ to be smooth. We give an example of this phenomenon.

Example:

Using the construction from Jeon, Kim & Lee (2011), let us take a rational curve with torsion $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ over the field $\mathbb{K} = \mathbb{Q}(\sqrt{-3}, \sqrt{217})$ and torsion $\mathbb{Z}/6\mathbb{Z}$ over $\mathbb{Q}$. The curve is:

$$E_1 : y^2 = x^3 - 17811145/19683x - 81827811574/14348907.$$

Now take

$$E_2 : y^2 = x^3 - 25081083x + 44503996374.$$

The torsion of $E_2(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/7\mathbb{Z}$, implying that by standard heuristics (examining only the rational torsion), $|E_2(\mathbb{F}_p)|$ should be more often smooth than $|E_1(\mathbb{F}_p)|$. Note that both curves have rank 1 over $\mathbb{Q}$, so the rank should not play a role.

We examine how often $|E_i(\mathbb{F}_{p_n})|$, $i = 1, 2$, are 100-smooth and 200-smooth, where p_n is the $n-$th prime number, runs through the first 10000 and 100000 primes, excluding the first ten primes (to get rid of the primes of bad reduction). For comparison, we also take the elliptic curve

$$E_3 : y^2 = x^3 + 3,$$

with a trivial torsion group and rank 1.

	$10 < n < 10010$	$10 < n < 100010$
#100-sm. $\lvert E_1(\mathbb{F}_{p_n})\rvert$	4843	22872
#100-sm. $\lvert E_2(\mathbb{F}_{p_n})\rvert$	4302	20379
#100-sm. $\lvert E_3(\mathbb{F}_{p_n})\rvert$	2851	12344
#200-sm. $\lvert E_1(\mathbb{F}_{p_n})\rvert$	6216	35036
#200-sm. $\lvert E_2(\mathbb{F}_{p_n})\rvert$	5690	32000
#200-sm. $\lvert E_3(\mathbb{F}_{p_n})\rvert$	4134	21221

We see that, contrary to what one would expect if examining only the rational torsion, E_1 is consistently more likely to be smooth than E_2. Why does this happen? Examine the behavior of the torsion of $E_1(\mathbb{K})$ and $E_2(\mathbb{K})$ as $\mathbb{K}$ varies through all quadratic fields. The torsion of $E_2(\mathbb{K})$ will always be $\mathbb{Z}/7\mathbb{Z}$, while $E_1(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and $E_1(\mathbb{Q}(\sqrt{217}))_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. One fourth of the primes will split in $\mathbb{Q}(\sqrt{-3})$ and not in $\mathbb{Q}(\sqrt{217})$, one fourth vice versa, one fourth will split in neither field and one fourth will split in both fields (and thus splitting completely in $\mathbb{Q}(\sqrt{-3}, \sqrt{217})$). This implies that we know that $|E_1(\mathbb{F}_p)|$ is divisible by 6, 12, 18 and 36, each for one fourth of the primes, while all we can say for $|E_2(\mathbb{F}_p)|$ is that it is divisible by 7. We also see that $|E_3(\mathbb{F}_p)|$ is much less likely to be smooth than both E_1 and E_2.

Nice explicit examples of factorization of large numbers (Cunningham numbers in this case) by using elliptic curves over number fields of small degree have been provided recently by **Brier and Clavier (2010)**. These authors used elliptic curves over cyclotomic fields with torsion groups $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. E.g. they found a factor

5546025484206613872527377154544456740766039233

of $2^{1048} + 1$ and a factor

1581214773543289355763694808184205062516817

of $2^{972} + 1$.

Also, they tried to construct elliptic curves over cyclotomic fields with torsion $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ and positive rank, but failed.

Recently, we were able to find such curves over quartic fields.

Bosman, Bruin, Dujella and Najman (2012):

The elliptic curve

$y^2 = x^3 - (67950603/100000000)x - 63221225949/500000000000$

has torsion group $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ and a point of infinite order $(-3549/10000, 1323/5000)$ over $\mathbb{Q}(i, \sqrt{7})$.

The elliptic curve

$$y^2 - (88/93)xy - (181/93)y = x^3 - (181/93)x^2$$

has torsion group $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}5\mathbb{Z}$ and a point of infinite order $(2/3, 7/3)$ over $\mathbb{Q}(\zeta_5)$, where ζ_5 is a fifth root of unity.