Elliptic curves with large torsion and positive rank over number fields of small degree and ECM factorization

Andrej Dujella and Filip Najman

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

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 infinite cyclic group:

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

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

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

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)

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

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)

High-rank elliptic curves with some other additional properties:

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

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

- 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)

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

Elliptic curves over quadratic fields

Kenku & Momose (1988), Kamienny (1992):
Let E be an elliptic curve over a quadratic field K. The torsion group of $E(K)$ 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 $K = \mathbb{Q}(\sqrt{-3})$);
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (only if $K = \mathbb{Q}(i)$).

Note that if torsion group over a number field K contains $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, then the m-th roots of unity lie in 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 $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

A. D. & F. N. (2011):
There exist elliptic curves over quadratic fields with positive rank and torsion $\mathbb{Z}/15\mathbb{Z}$ (rank ≥ 1 over $\mathbb{Q}(\sqrt{345})$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ (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, except maybe for $\mathbb{Z}/18\mathbb{Z}$.

It seems that all such curves with torsion $\mathbb{Z}/18\mathbb{Z}$ have even rank (this is work in progress – J. Bosman, P. Bruin, A. D. & F. N.).

Similar results for cubic and quartic fields.

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? **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 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 $p | \gcd(a^m - 1, n)$. 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.

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

$$5546025484206613872527377154544567 40766039233$$

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.

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

$$y^2 = x^3 - (15278701/3)x + 76661239672475/108$$

has torsion group $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}5\mathbb{Z}$ and a point of infinite order $(2401/3, 1680789/2)$ over $\mathbb{Q}(\zeta_5)$, where ζ_5 is a fifth root of unity.

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 $E(\mathbb{Q})_{\mathsf{tors}}$ 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 1.

Using the construction from Jeon, Kim and Lee (2011), let us take a rational curve with torsion $\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$ over the field $K = \mathbb{Q}(\sqrt{-3}, \sqrt{217})$ 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 $E_1(K)$ and $E_2(K)$ as K varies through all quadratic fields. The torsion of $E_2(K)$ 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.