New rank records for elliptic curves with rational torsion

ANTS-14, New Zoomland 6–7/2020

Noam D. Elkies*[1] & Zev Klagsbrun[2]

1) Harvard University, Cambridge, MA USA

2) Center for Communications Research, La Jolla, CA USA

Overview

- Elliptic curves $E/\mathbf{Q}$: theorems of Mordell[–Weil] and Mazur
- General approach: find E_t, search for good specializations t
- Mestre-Nagao heuristic and new improvements
- New results

An *elliptic curve* E over $\mathbf{Q}$ is a smooth cubic curve in $\mathbf{P}^2$ with rational coefficients and a rational point.

It is well known that there is a choice of coordinates x, y that puts E in "Weierstrass form" $y^2 = x^3 + ax + b$; the rational points are then the solutions $(x, y) \in \mathbf{Q}^2$ of the Diophantine equation $y^2 = x^3 + ax + b$, together with the "point at infinity" $\mathbf{0}$: $(x : y : 1) = (0 : 1 : 0)$. The curve is smooth *iff* the discriminant $\Delta = 4a^3 + 27b^2$ is nonzero.

It's often more convenient to use "extended Weierstrass form"

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

abbreviated to just the vector $(a_1, a_2, a_3, a_4, a_6)$ of coefficients. We may assume $a_i \in \mathbf{Z}$ because

$$(x, y; a_1, a_2, a_3, a_4, a_6) \cong (c^2x, c^3y; ca_1, c^2a_2, c^3a_3, c^4a_4, c^6a_6).$$

An *elliptic curve* E over $\mathbf{Q}$ is a smooth cubic curve in $\mathbf{P}^2$ with rational coefficients and a rational point.

It is well known that there is a choice of coordinates x, y that puts E in "Weierstrass form" $y^2 = x^3 + ax + b$; the rational points are then the solutions $(x, y) \in \mathbf{Q}^2$ of the Diophantine equation $y^2 = x^3 + ax + b$, together with the "point at infinity" $\mathbf{0}$: $(x : y : 1) = (0 : 1 : 0)$. The curve is smooth *iff* the discriminant $\Delta = 4a^3 + 27b^2$ is nonzero.

It's often more convenient to use "extended Weierstrass form"

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

abbreviated to just the vector $(a_1, a_2, a_3, a_4, a_6)$ of coefficients. We may assume $a_i \in \mathbf{Z}$ because

$$(x, y; a_1, a_2, a_3, a_4, a_6) \cong (c^2x, c^3y; ca_1, c^2a_2, c^3a_3, c^4a_4, c^6a_6).$$

Theorem [Mordell 1922]:
$E(\mathbf{Q})$ *is a finitely generated abelian group.*

That is, $E(\mathbf{Q}) \cong E(\mathbf{Q})_{\text{tors}} \oplus \mathbf{Z}^r$, where $E(\mathbf{Q})_{\text{tors}}$ is a finite abelian group and $0 \le r < \infty$. This r is the *rank* of E.

Fundamental question: which pairs (G, r) occur as $(E(\mathbf{Q})_{\text{tors}}, \text{rank}(E))$ for some (or infinitely many) $E/\mathbf{Q}$?

Mazur's torsion theorem (1977):
$E(\mathbf{Q})_{\text{tors}}$ *is always isomorphic with either* $\mathbf{Z}/n\mathbf{Z}$ *(some* $n \le 10$ *or* $n = 12$*) or* $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2n\mathbf{Z})$ *(some* $n \le 4$*).*

Each of these $11 + 4$ groups G occurs for infinitely many E.

Theorem [Mordell 1922]:
$E(\mathbf{Q})$ *is a finitely generated abelian group.*

That is, $E(\mathbf{Q}) \cong E(\mathbf{Q})_{\text{tors}} \oplus \mathbf{Z}^r$, where $E(\mathbf{Q})_{\text{tors}}$ is a finite abelian group and $0 \leq r < \infty$. This r is the *rank* of E.

Fundamental question: which pairs (G, r) occur as $(E(\mathbf{Q})_{\text{tors}}, \text{rank}(E))$ for some (or infinitely many) $E/\mathbf{Q}$?

Mazur's torsion theorem (1977):
$E(\mathbf{Q})_{\text{tors}}$ *is always isomorphic with either* $\mathbf{Z}/n\mathbf{Z}$ *(some* $n \leq 10$ *or* $n = 12$*) or* $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2n\mathbf{Z})$ *(some* $n \leq 4$*).*

Each of these $11 + 4$ groups G occurs for infinitely many E.

Theorem [Mordell 1922]:
$E(\mathbf{Q})$ *is a finitely generated abelian group.*

That is, $E(\mathbf{Q}) \cong E(\mathbf{Q})_{\text{tors}} \oplus \mathbf{Z}^r$, where $E(\mathbf{Q})_{\text{tors}}$ is a finite abelian group and $0 \le r < \infty$. This r is the *rank* of E.

Fundamental question: which pairs (G, r) occur as $(E(\mathbf{Q})_{\text{tors}}, \text{rank}(E))$ for some (or infinitely many) $E/\mathbf{Q}$?

Mazur's torsion theorem (1977):
$E(\mathbf{Q})_{\text{tors}}$ *is always isomorphic with either* $\mathbf{Z}/n\mathbf{Z}$ *(some* $n \le 10$ *or* $n = 12$*) or* $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2n\mathbf{Z})$ *(some* $n \le 4$*).*

Each of these $11 + 4$ groups G occurs for infinitely many E.

[Repeat] **Mazur's torsion theorem** (1977):
$E(\mathbf{Q})_{\text{tors}}$ is always isomorphic with either $\mathbf{Z}/n\mathbf{Z}$ (some $n \leq 10$ or $n = 12$) or $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2n\mathbf{Z})$ (some $n \leq 4$).

Each of these $11 + 4$ groups G occurs for infinitely many E.

For example, $(0,0,0,1,0) : y^2 = x^3 + x$ (from Fermat's proof of FLT_4), or generally

$$(0, a_2, 0, a_4, 0) : y^2 = x^3 + a_2x^2 + a_4x,$$

has a 2-torsion point at $(0,0)$; and $y^2 + y = x^3$ (from Euler's proof of FLT_3), or generally

$$(a_1, 0, a_3, 0, 0) : y^2 + a_1xy + a_3y = x^3,$$

has a 3-torsion point, again at $(0,0)$. For most $a_i \in \mathbf{Q}$ these give $E(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Z}/3\mathbf{Z}$ respectively.

Randomly chosen coeffs a_i almost always yield $E(\mathbf{Q})_{\text{tors}} = \{0\}$, but in practice curves with nontrivial torsion arise often, as with FLT_3 and FLT_4. Torsion also tends to make r and $E(\mathbf{Q})$ easier to determine by “descent”, again as with FLT_3 and FLT_4. Both of those curves have $r = 0$; an example with large rank is

🍌 + 🍎 + 🍊 = 977315089699,

🍌 × 🍎 × 🍊 = 283424925213\
932974760115972230625

with torsion $\mathbf{Z}/3\mathbf{Z}$ and rank 14 (E., 2018).

[In general $X + Y + Z = a_1$, $XYZ = a_3$ gives $(a_1, 0, a_3, 0, 0)$; translation by 3-torsion cyclically permutes $\{X, Y, Z\}$.]

So the natural question now is:

`Given one of the fifteen groups` G `in Mazur's list, how large can` r `get for an elliptic curve` $E/\mathbf{Q}$ `with` $E(\mathbf{Q}) \cong G \oplus \mathbf{Z}^r$`?`

We report on new searches for such E, and in particular on new records for five of the fiften groups G, namely the cyclic groups of orders $2, 3, 4, 6, 7$.

For example, we increment the $G = \mathbf{Z}/3\mathbf{Z}$ record to

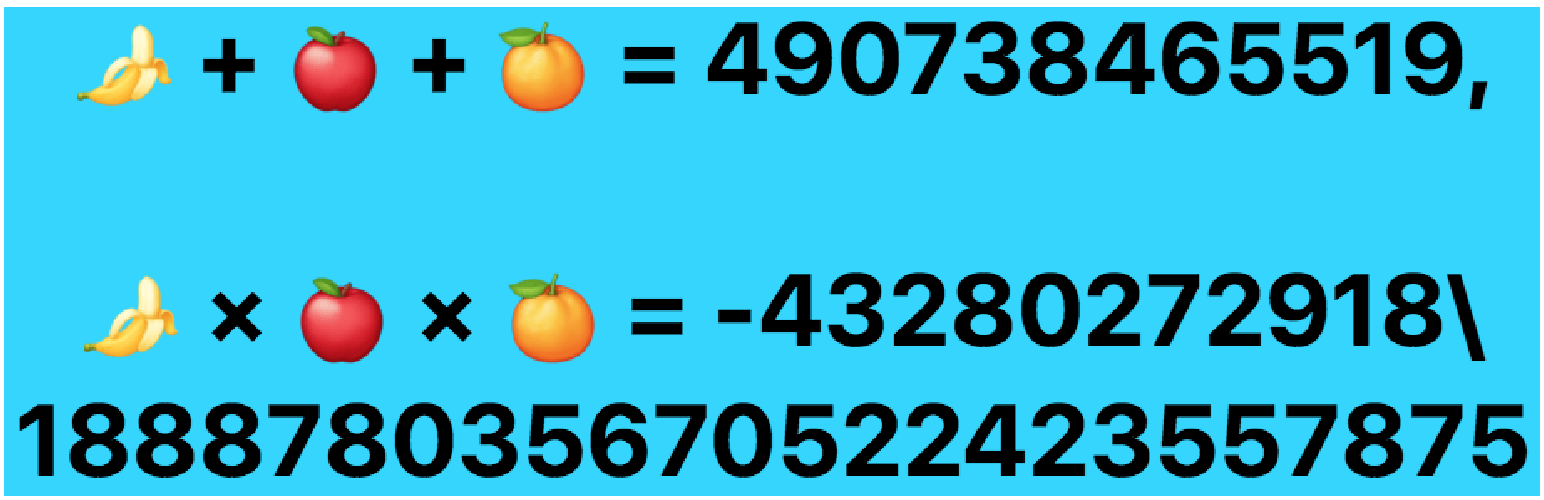
with torsion $\mathbf{Z}/3\mathbf{Z}$ and rank 15.

So the natural question now is:

`Given one of the fifteen groups` G `in Mazur's list, how large can` r `get for an elliptic curve` $E/\mathbf{Q}$ `with` $E(\mathbf{Q}) \cong G \oplus \mathbf{Z}^r$`?`

We report on new searches for such E, and in particular on new records for five of the fiften groups G, namely the cyclic groups of orders $2, 3, 4, 6, 7$.

For example, we increment the $G = \mathbf{Z}/3\mathbf{Z}$ record to



with torsion $\mathbf{Z}/3\mathbf{Z}$ and rank 15.

Table showing the new r records for $G = \mathbf{Z}/n\mathbf{Z}$ $(n = 2, 3, 4, 6, 7)$,
From `https://web.math.pmf.unizg.hr/~duje/tors/tors.html` :

$E(\mathbf{Q})_{\text{tors}}$	previous record	current record
$\{1\}$	28 (E., 2006)	
$\mathbf{Z}/2\mathbf{Z}$	19 (E., 2009)	20 (E.-K.)
$\mathbf{Z}/3\mathbf{Z}$	14 (E., 2018)	15 (E.-K.)
$\mathbf{Z}/4\mathbf{Z}$	12 (E., 2006)	13 (E.-K.)
$\mathbf{Z}/5\mathbf{Z}$	8 (Dujella-Lecacheux, 2009)	
$\mathbf{Z}/6\mathbf{Z}$	8 (Eroshkin, 2008)	9 (K.)
$\mathbf{Z}/7\mathbf{Z}$	5 (Dujella-Kulesz, 2001)	6 (K.)
$\mathbf{Z}/8\mathbf{Z}$	6 (E., 2006)	
$\mathbf{Z}/9\mathbf{Z}$	4 (Fisher, 2009)	
$\mathbf{Z}/10\mathbf{Z}$	4 (Dujella, 2005)	
$\mathbf{Z}/12\mathbf{Z}$	4 (Fisher, 2008)	
$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2\mathbf{Z})$	15 (E., 2009)	
$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z})$	9 (Dujella-Peral, 2012)	
$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/6\mathbf{Z})$	6 (E., 2006)	
$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/8\mathbf{Z})$	3 (Connell, 2000)	

Table showing the new r records for $G = \mathbf{Z}/n\mathbf{Z}$ $(n = 2, 3, 4, 6, 7)$,
From `https://web.math.pmf.unizg.hr/~duje/tors/tors.html` :

$E(\mathbf{Q})_{\mathrm{tors}}$	previous record		current record
$\{1\}$	28	(E., 2006)	28
$\mathbf{Z}/2\mathbf{Z}$	19	(E., 2009)	**20 (E.-K.)**
$\mathbf{Z}/3\mathbf{Z}$	14	(E., 2018)	**15 (E.-K.)**
$\mathbf{Z}/4\mathbf{Z}$	12	(E., 2006)	**13 (E.-K.)**
$\mathbf{Z}/5\mathbf{Z}$	8	(Dujella-Lecacheux, 2009)	8
$\mathbf{Z}/6\mathbf{Z}$	8	(Eroshkin, 2008)	**9 (K.)**
$\mathbf{Z}/7\mathbf{Z}$	5	(Dujella-Kulesz, 2001)	**6 (K.)**
$\mathbf{Z}/8\mathbf{Z}$	6	(E., 2006)	6
$\mathbf{Z}/9\mathbf{Z}$	4	(Fisher, 2009)	4
$\mathbf{Z}/10\mathbf{Z}$	4	(Dujella, 2005)	4
$\mathbf{Z}/12\mathbf{Z}$	4	(Fisher, 2008)	4
$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2\mathbf{Z})$	15	(E., 2009)	15
$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z})$	9	(Dujella-Peral, 2012)	9
$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/6\mathbf{Z})$	6	(E., 2006)	6
$(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/8\mathbf{Z})$	3	(Connell, 2000)	3

The new curve with $E(\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z}) \oplus \mathbf{Z}^{20}$ now also holds the record for the largest rank of $E(\mathbf{Q})$ for an elliptic curve E whose rank is known unconditionally (i.e., not assuming any GRH).

Other Results: for the same G's (cyclic of orders 2,3,4,6,7) and a few others, we find numerous new examples of E that tie the previous rank records for $E(\mathbf{Q})_{\text{tors}} \cong G$, including a few that are smaller* than any previously known with the same $(E(\mathbf{Q})_{\text{tors}}, r)$.

* "Smaller" may be measured by height, discriminant, and/or conductor.

Overview of search technique. The overall strategy for such searches has not changed in decades:

i) Find a family $\{E_t\}$ with $G \oplus \mathbf{Z}^{r_0} \hookrightarrow E_t$ for almost all t;
ii) Search for special values of $t \in \mathbf{Q}$ (or $t \in \mathbf{Q}^d$, etc.) for which E_t has even more rational points.

A simple example of (i) for $|G| = r_0 = 2$: let $t = (x_1, y_1, x_2, y_2) \in \mathbf{Q}^4$; solve simult. lin. eqs. $y_i^2 = x_i^3 + a_2 x_i^2 + a_4 x_i$ $(i = 1, 2)$ for (a_2, a_4). (For $G = \mathbf{Z}/2\mathbf{Z}$ we actually used E_t with $r_0 = 9$; the construction of such E_t is described elsewhere.)

Our new improvements all target part (ii).

Mestre-Nagao heuristic for good candidates E_t.

Wholesale testing of curves E_t for high rank is usually not feasible. Instead one uses the heuristic of Mestre (1982) and Nagao (1992): record and near-record rank curves E tend to have many points modulo most small primes p. So use a score

$$S(t,B) := \log \prod_{p \le B} \frac{N_p(E_t)}{p} = \sum_{p \le B} \log \frac{N_p(E_t)}{p}$$

as a proxy for high rank. Here p ranges over "primes of good reduction" for the curve ($p \nmid \Delta$), and $N_p(E_t) = \#E_t(\mathbf{Z}/p\mathbf{Z})$, which is easy to compute for small p.

[This score also aligns with the BSD conjecture: $\prod_{p \le B} N_p(E)/p$ is a partial product for $1/L(E,1)$.]

Sieving for bulk computation of $S(t, B)$.

We now use a trick known from "Sieve" techniques (QS, NFS) for factoring etc. to efficiently compute many values of

$$S(t, B) = \sum_{p \le B} \log \frac{N_p(E_t)}{p}.$$

That is:

- Set up an array of counters s_t, initialized to zero

- For each $p \le B$: for each τ mod p: compute $\log(N_p(E_\tau)/p)$, and use it to increment each s_t in the arith. prog. $t \equiv \tau \bmod p$.

This make $s_t = S(t, B)$ for each t.

[In practice, fix $M = 2^{10}$, compute $\texttt{ROUND}(M \log(N_p(E_\tau)/p))$, and approximate $M \cdot S(t, B)$ by the 16-bit sum of those integers.]

Post-sieve processing

Having computed many approximate $S(t, B)$ values, take the top "few" for further processing: possibly compute $S(t, B')$ for some $B' \gg B$ to further cull the list, then descent* to get upper bound on rank of E_t, and if the bound is large enough then search for rational points.

* 2-descent for $n = 5$ or $n = 7$; descent by 2- or 3-isogeny otherwise. For 3-isogeny, also implemented Cassels–Tate pairing.

A decisive ingredient for all the new records (except maybe $G = \mathbf{Z}/7\mathbf{Z}$) was throwing *lots* more computing power at the problem. All of Elkies' previous rank-record curves took less than half a core-year in total. Here each of $\mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Z}/3\mathbf{Z}$ got 40+ core-years, $\mathbf{Z}/6\mathbf{Z}$ got almost that much, and $\mathbf{Z}/4\mathbf{Z}$ got about 12. Klagsbrun also searched the universal $\mathbf{Z}/5\mathbf{Z}$ family $[t+1, t, t, 0, 0]$ for several core-*centuries*; so far the record rank remains 8 (Dujella-Lecacheux), but now with 100+ new examples, including the smallest conductor and discriminant known for a curve with $E(\mathbf{Q}) \cong (\mathbf{Z}/5\mathbf{Z}) \oplus \mathbf{Z}^8$, at $t = 1809535/5292661$ and $t = 5167107/723695$ respectively (conductor $\approx 2^{85.86}$, resp. discriminant $\approx 2^{254.77}$).

Further work along these lines will resume once our world is back to some semblance of normality ...

A decisive ingredient for all the new records (except maybe $G = \mathbf{Z}/7\mathbf{Z}$) was throwing *lots* more computing power at the problem. All of Elkies' previous rank-record curves took less than half a core-year in total. Here each of $\mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Z}/3\mathbf{Z}$ got 40+ core-years, $\mathbf{Z}/6\mathbf{Z}$ got almost that much, and $\mathbf{Z}/4\mathbf{Z}$ got about 12. Klagsbrun also searched the universal $\mathbf{Z}/5\mathbf{Z}$ family $[t+1, t, t, 0, 0]$ for several core-*centuries*; so far the record rank remains 8 (Dujella-Lecacheux), but now with 100+ new examples, including the smallest conductor and discriminant known for a curve with $E(\mathbf{Q}) \cong (\mathbf{Z}/5\mathbf{Z}) \oplus \mathbf{Z}^8$, at $t = 1809535/5292661$ and $t = 5167107/723695$ respectively (conductor $\approx 2^{85.86}$, resp. discriminant $\approx 2^{254.77}$).

Further work along these lines will resume once our world is back to some semblance of normality . . .