New elliptic curves of large rank and low conductor

[preliminary report]

JMM $7 \times 17 \times 17 = \binom{24}{3} - 1$, Boston, 4 January 2023

Special Session: arithmetic geometry informed by computation

Noam D. Elkies, Harvard University

Elliptic curves over $\mathbf{Q}$: Review and context

Elliptic curve: a Dioph. equation

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

$a_i \in \mathbf{Q}$ (and $\exists$ model with $a_i \in \mathbf{Z}$), $\Delta \neq 0$
(e.g. $4a_4^3 + 27a_6^2 \neq 0$ for $y^2 = x^3 + a_4x + a_6$).

THEOREM (Mordell 1922): *The rational solutions* (x, y), *together with "point at* ∞*", form an abelian group with identity* ∞.

This group $E(\mathbf{Q})$ *is finitely generated.*

So, $E(\mathbf{Q}) \cong T \oplus \mathbf{Z}^r$ for some finite torsion group $T = (E(\mathbf{Q}))_{\text{tors}}$ and finite r.

What (T, r) can arise?

For T, the question is completely settled:

THEOREM (Mazur 1977–78): *Every $E/\mathbf{Q}$ has either*

- $E(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/n\mathbf{Z}$ *for some* $n \leq 10$ *or* $n = 12$, *or*
- $E(\mathbf{Q})_{\text{tors}} \cong (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2n\mathbf{Z})$ *for some* $n \leq 4$.

Each of those 15 groups (cyclic of order $1, \ldots, 10$ or 12, or $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2n\mathbf{Z})$ for $n = 1, 2, 3, 4$) arises infinitely often. For example, $E(\mathbf{Q})_{\text{tors}}$ contains $(\mathbf{Z}/2\mathbf{Z})$, $(\mathbf{Z}/3\mathbf{Z})$, $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2\mathbf{Z})$ iff E can be written as

$$y^2 = x^3 + a_2x^2 + a_4x,$$
$$y^2 + a_1xy + a_3y = x^3,$$
$$y^2 = (x - e)(x - e')(x - e'')$$

respectively.

So:

Given T, what are the possible ranks r of $E/\mathbf{Q}$ with $E(\mathbf{Q})_{\text{tors}} \cong T$?

That's still open; even the right guess is disputed . . .

Current rank records

(from https://web.math.pmf.unizg.hr/∼duje/tors/tors.html)

T	r [each $r' < r$ is known too]
1	28* [NDE 2006]
2	20 [NDE–ZK 2020] (K = Klagsbrun)
3	15 [NDE–ZK 2020]
4	13 [NDE–ZK 2020]
5	9 [ZK 2020]
6	9 [ZK 2020]
7	6 [ZK 2020]
8	6 [NDE 2006]
9	4 [TF 2009] (F = Fisher)
10	4 [AD 2005] (D = Dujella)
12	4 [TF 2008]
2×2	15 [NDE 2009]
2×4	9 [AD–JCP 2012] (P = Peral)
2×6	6 [NDE 2006]
2×8	3 [IC 2000] (C = Connell)

Seeking simple (T, r) curves

I bear no further news about such rank records.
Our topic today is in another direction:

Given T and $r = 0, 1, 2, \ldots$, how simple an E can we find s.t. $E(\mathbf{Q})$ is (or contains) $T \oplus \mathbf{Z}^r$?

"Simple" can be small conductor N, abs.disc. $|\Delta|$, or height H ($|a_i| \ll H^i$, $i \in \{1, 2, 3, 4, 6\}$).

["(or contains)" avoids $r = 0$ anomalies like $E = \mathsf{X}_1(11) : y^2 + y = x^3 - x^2$ with $|T| = 5$; "$\mathsf{X}_2(11)$": $y^2 + y = x^3 - x^2 - 7820x - 263580$ has $E(\mathbf{Q}) = \{\infty\}$ and $N = 11$ but doesn't look "simple"...]

LMFDB (currently $N < 5 \cdot 10^5$, $N \mid 2^8 3^5 5^2 7^2 = 76\,204\,800$, and $N < 3 \cdot 10^8$ prime) answers this only for $r \leq 5$ with $|T| = 1^*$:

r	$N_{\min}$	E
1	37	$y^2 + y = x^3 - x$
2	389	$y^2 + y = x^3 + x^2 - 2x$
3	5077	$y^2 + y = x^3 - 7x + 6$
4	234446	$y^2 + xy = x^3 - x^2 - 79x + 289$ [NB $D = 2N < 501029$]
5	19047851	$y^2 + y = x^3 - 79x + 342$

And at most 3 for $|T| \geq 2$, e.g. $N_{\min}$ for $|T| < 4$ is:

r	$\mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/3\mathbf{Z}$	$(\mathbf{Z}/2\mathbf{Z})^2$	$\mathbf{Z}/4\mathbf{Z}$
1	65	91	117	117
2	1088	1862	2175	2175
3	59450	201042	174915	217328

(*) Minimal height might be different, e.g. $r = 4$ for $y^2 + y = x^3 - 7x + 36$ with $N = 545723$. For $r = 5$ there may be smaller composite N.

For $|T| = 1$, we [NDE & Mark Watkins, 2004 (ANTS-6, arXiv:math.NT/0403374)] found candidate curves for $r \leq 11$; e.g. our smallest N are:

r	N	$[a_1, a_2, a_3, a_4, a_6]$
5	19047851	$[0, 0, 1, -79, 342]$
6	5187563742	$[1, 1, 0, -2582, 48720]$
7	382623908456	$[0, 0, 0, -10012, 346900]$
8	249649566346838	$[1, -1, 0, -106384, 13075804]$
9	32107342006814614	$[1, -1, 0, -135004, 97151644]$
10	10189285026863130793	$[0, 0, 1, -16312387, 25970162646]$
11	1803173772593563652084 3	$[0, 0, 1, -16359067, 26274178986]$

(the $r = 10$ record has $|\Delta| = 11^3 N$; the curve with $[a_1, \ldots, a_6] = [1, -1, 0, -1536664, 648294124]$ has rather smaller H and $|\Delta|$).

New results

In last Boston JMM (2012) we [=NDE] suggested how we might search more efficiently. Finally doing this a decade later, we find:

- Candidates for $r = 12$ and $r = 13$; the table grows to:

r	N	$[a_1, a_2, a_3, a_4, a_6]$
6	5187563742	$[1, 1, 0, -2582, 48720]$
7	382623908456	$[0, 0, 0, -10012, 346900]$
8	249649566346838	$[1, -1, 0, -106384, 13075804]$
9	3210734200681461 4	$[1, -1, 0, -135004, 97151644]$
10	10189285026863130793	$[0, 0, 1, -16312387, 25970162646]$
11	18031737725935636520843	$[0, 0, 1, -16359067, 26274178986]$
12	26145292874820119408329144	$[0, 0, 0, -932733487, 110523541472 50]$
13	38252643743425234347938185256	$[0, 0, 0, -6529826212, 195995662948900]$

Also new runners-up, though no new records, for some $r \leq 11$.

• For the first time, candidate "simplest curves" for several nontrivial T and ranks beyond LMFDB range.

Example: $T = \mathbf{Z}/3\mathbf{Z}$, with curves $[a_1, 0, a_3, 0, 0]$ (that is, $y^2 + a_1xy + a_3y = x^3$), which have 3-torsion at $(0, 0)$:

r	N	(a_1, a_3)
4	15913354	$(-19, 6016)$
5	3492684130	$(169, 50375)$
6	9730454816874	$(-1171, 116671104)$
7	10190734612809870	$(2821, 361060875)$
8	867543430767396342 54	$(-16633, 50306635008)$
9	266361669235181498791 9950	$(-19215, 1131830787360)$

(Happily for $r = 3$ the $N = 201042$ curve did appear; likewise for the other optimal curves in the LMFDB.)

Also: $y^2 = x(x - 283816167936)(x - 305457034575)$ gives $(T, r) = ((\mathbf{Z}/2\mathbf{Z})^2, 10)$ with $N \simeq 3.6735 \cdot 10^{27}$, "etc."

The approach of [NDE–Watkins 2004]

We could not approach $r = 11$ by searching all E up to height H: too many such ($\sim H^{4+6} = H^{10}$).

Heuristic: Record curves generated by small integral points. Search for (E, P_1). Choose $x_1, y_1, a_4 \ll H^2, H^3, H^4$, and solve

$$y_1^2 + a_1 x_1 y_1 + a_3 y_1 = x_1^3 + a_2 x_1^2 + a_4 x_1 + a_6$$

for a_6. Now "only" $\sim H^{2+3+4} = H^9$ candidates. For each a_1, a_2, a_3 and a_4, check all a_6 that appear many times.

But H^9 is still a lot. So, search for (E, P_1, P_2). E.g., if $a_1 = a_2 = a_3 = 0$, given (x_1, x_2, y_1, y_2), solve for (a_4, a_6), which are integral iff

$$x_1 - x_2 \mid y_1^2 - y_2^2 = (y_1 - y_2)(y_1 + y_2)$$

and we're down to $\sim H^8 \log H$ — and much more bookkeeping.

$H^{8+\epsilon}$ down to H^5

We expect at least H^{10-k} marked curves $(E, P_1, \ldots, P_k)$ with indept. integral P_i, but already for $k = 3$ it's hard to find and work with a complete parametrization.

But for small k it's much simpler — and still H^{10-k} — to work with $(E, P_1, \ldots, P_k)$ satisfying extra integrality condition. Consider $r = 2$, and require P, P', P'' integral and collinear, so $P + P' + P'' = 0$. If the line is $y = \alpha_1 x + \alpha_3$ then

$$x(P) + x(P') + x(P'') = \alpha_1^2 + a_1\alpha_1 - a_2$$

so $\alpha_1 \in \mathbf{Z}$, and then also $\alpha_3 \in \mathbf{Z}$ and we've parametrized $(E, P, P', P'' \mid P + P' + P'')$ by $\alpha_1, \alpha_3, x(P), x(P')$ so a total of $\sim H^{1+3+2+2} = H^8$ candidates.

Geometrically*: moduli space $\mathcal{M}_{1,3}$ of genus-1 curves with 3 distinct pts. P_i, such as $0, P, -P'$. (Since $P_i \neq P_j$ at every prime means $P_i - P_j \neq 0 \Leftrightarrow x(P_i - P_j) \neq \infty$ at all p, so $P_i - P_j$ integral!) Can parametrize $\mathcal{M}_{1,k+1}$ for $k \leq 5$: weighted $\mathbf{P}^{k+1}$ with weights $(2,3,4)$, $(1,2,2,3)$, $(1,1,1,2,2)$, $(1,1,1,1,1,1)$ for $k = 1,2,3,4$; for $k = 5$: Grassmannian of lines in $\mathbf{P}^4$! Once $k \geq 6$, singular and less accessible; but already $k = 5$ gives H^5, much better than H^8.

For $|T| > 1$, we use a slice of $\mathcal{M}_{1,|T|(k+1)}$ where T acts on the $|T|(k+1)$ points. Some nice models here too, e.g. $\mathbf{P}^2 \times \mathbf{P}^2$ for $(|T|,k) = (2,3)^*$ (reducing H^6 to $H^3 \log H$), and $\mathbf{P}^3$ for $(T,k) = ((\mathbf{Z}/2\mathbf{Z})^2, 2)$ (H^4 to $H^2 \log^2 H$).

(*) Thanks to Eric Rains for making this connection and noting previous work [Smyth 2011 (Compos. Math.), Lekili–Polishchuk 2014 (arXiv:1408.0611)], Grassmannian model for $k = 5$, ... and $\mathbf{P}^2 \times \mathbf{P}^2$ model for $(|T|,k) = (2,3)$.

Geometrically*: moduli space $\mathcal{M}_{1,3}$ of genus-1 curves with 3 distinct pts. P_i, such as $0, P, -P'$. (Since $P_i \neq P_j$ at every prime means $P_i - P_j \neq 0 \Leftrightarrow x(P_i - P_j) \neq \infty$ at all p, so $P_i - P_j$ integral!) Can parametrize $\mathcal{M}_{1,k+1}$ for $k \leq 5$: weighted $\mathbf{P}^{k+1}$ with weights $(2,3,4)$, $(1,2,2,3)$, $(1,1,1,2,2)$, $(1,1,1,1,1,1)$ for $k = 1,2,3,4$; for $k = 5$: Grassmannian of lines in $\mathbf{P}^4$! Once $k \geq 6$, singular and less accessible; but already $k = 5$ gives H^5, much better than H^8.

For $|T| > 1$, we use a slice of $\mathcal{M}_{1,|T|(k+1)}$ where T acts on the $|T|(k+1)$ points. Some nice models here too, e.g. $\mathbf{P}^2 \times \mathbf{P}^2$ for $(|T|, k) = (2,3)^*$ (reducing H^6 to $H^3 \log H$), and $\mathbf{P}^3$ for $(T, k) = ((\mathbf{Z}/2\mathbf{Z})^2, 2)$ (H^4 to $H^2 \log^2 H$).

(*) Thanks to Eric Rains for making this connection and noting previous work [Smyth 2011 (Compos. Math.), Lekili–Polishchuk 2014 (arXiv:1408.0611)], Grassmannian model for $k = 5$, and $\mathbf{P}^2 \times \mathbf{P}^2$ model for $(|T|, k) = (2,3)$.

So: for each of our parametrizations,

- pick H,
- compute E for all parameter values of height $\leq H$, then
- compute an approximate Mestre-Nagao product — actually an approximate logarithm $\sum_{p \leq X} \log((p+1-a_p)/p)$ — and send the top scorers to further testing:
- use ellratpoints to list small integral points, and
- compute the rank of the group they generate, adding 1 if the parity conjecture requires it.

Still to be done:

- Tricks to get at some T indirectly (e.g. 2×4 from either 2×2 or 4),
- Refine $(|T|, k) = (1, 5)$ to catch odd-N curves directly (NB: good reduction at $2 \Rightarrow E$ mod 2 can't have 6 distinct points!);
- Massive runs, extensive statistics

So: for each of our parametrizations,

• pick H,

• compute E for all parameter values of height $\leq H$, then

• compute an approximate Mestre-Nagao product — actually an approximate logarithm $\sum_{p \leq X} \log((p+1-a_p)/p)$ — and send the top scorers to further testing:

• use ellratpoints to list small integral points, and

• compute the rank of the group they generate, adding 1 if the parity conjecture requires it.

Still to be done:

• Tricks to get at some T indirectly (e.g. 2×4 from either 2×2 or 4),

• Refine $(|T|, k) = (1, 5)$ to catch odd-N curves directly (NB: good reduction at $2 \Rightarrow E$ mod 2 can't have 6 distinct points!);

• Massive runs, extensive statistics

THANK YOU