THE SMALLEST CONGRUENT NUMBER CURVE OF RANK SEVEN

OTAKHON U. KENJAEV

Abstract. Let $E_k\colon y^2 = x^3 - k^2x$. Rogers (2004) found that E_k has rank 7 for $k = 797507543735$, so the smallest such k (OEIS A194687, $a(7)$) is at most this number; minimality has been open. We prove that $a(7) = 797507543735$. The proof is an exhaustive, unconditional computation: a Monsky 2-Selmer sieve over all squarefree $k < 797507543735$, followed by Cassels-pairing upper bounds from PARI/GP `ellrank`, with isogeny-class refinement for the few residual cases and an independent cross-check with Cremona's `mwrank`. No hypothesis (GRH, BSD, parity) is used.

1. Statement

Theorem 1. *For every positive integer $k < 797507543735$ the curve E_k has rank at most 6. Hence $a(7) = 797507543735$.*

Lemma 2 (reduction to squarefree k)**.** *$E_{u^2k} \cong E_k$ over $\mathbb{Q}$ via $(x, y) \mapsto (u^2x, u^3y)$. Hence the smallest k with $\operatorname{rank} E_k \geq 7$ is squarefree.*

Checked numerically on 40 random pairs by comparing minimal models (`verify_all.py`, check 11).

2. Monsky sieve

For squarefree k with odd prime divisors $p_1, \dots, p_t$, Monsky's formula (as stated in Dujella–Janfada–Salami 2009, §3) gives the 2-Selmer rank $s(k) = 2t - \operatorname{rank}_{\mathbb{F}_2} M$, with $M = M_o$ or M_e built from Legendre symbols. Since $\operatorname{rank} E_k \leq s(k)$ and $s(k)$ is even iff $k \equiv 1, 2, 3 \pmod 8$, a curve of rank ≥ 7 needs $s(k) \geq 7$ ($k \equiv 5, 6, 7$) or $s(k) \geq 8$ ($k \equiv 1, 2, 3$); in particular $t \geq 4$. The rank parity conjecture is *not* used.

Completeness. The C sieve enumerates squarefree $k \leq N$ with $t \geq 4$ by depth-first search. Its count $T(N)$ is compared with an independent count $F(N) + F(N/2)$ computed from a prime-counting table (`pi_sanoq.c`):

N	$T(N)$ (sieve)	π-count
10^9	125034255	125034255
10^{10}	1455446848	1455446848
10^{11}	16432103801	16432103801
797507543734	143452705272	143452705272

Date: 29 September 2026 (version 1.0).

3. Elimination

Every candidate is passed to `ellrank` (PARI/GP 2.17.4, `nbthreads=1` because of a thread deadlock we observed), whose second output r_2 is an unconditional upper bound from 2-descent and the Cassels–Tate pairing.

range	candidates	max r_2	residual ($r_2 \geq 7$)
$\leq 10^{10}$	47796	5	0
$\leq 10^{11}$	804198	7	1
$(10^{11}, 797507543734]$	8249146	7	162

Residual cases. For $k = 85399368134 = 2 \cdot 19 \cdot 73 \cdot 4721 \cdot 6521$, `ellrank` gives $1 \leq r \leq 7$ (effort 6: $3 \leq r \leq 7$). The rank is an isogeny invariant; over the $\mathbb{Q}$-isogeny class (4 curves, `ellisomat`) the bounds are $r_2 = 7, 5, 5, 5$, so $\operatorname{rank} E_k \leq 5$. One curve of the class is $y^2 = x^3 + 4k^2x$. The same procedure applied to the 162 residual $k \in (10^{11}, 797507543734]$ gives $\min r_2$ over the isogeny class equal to 1 (11 cases), 3 (118 cases) and 5 (33 cases); none remains with $r_2 \geq 7$. Altogether all 9053344 candidates $k \leq 797507543734$ have $\operatorname{rank} E_k \leq 6$.

4. Independent cross-check

All candidates up to 10^{11} with $r_2 \geq 5$ (843 curves), 20 random candidates and the known values $a(5), a(6), a(7)$ were recomputed with Cremona's `mwrank` (eclib, via passagemath-eclib 10.8.12): 866/866 agree (no contradiction, no rank ≥ 7); $a(5), a(6), a(7)$ give ranks $5, 6, 7$ exactly. For $k \in (10^{11}, 797507543734]$ the same check was run on all 785 candidates with $r_2 \geq 6$ and 1000 random candidates, plus the three controls: 1788/1788 agree (no contradiction, no rank ≥ 7).

5. Reproducibility

All code, candidate lists and per-k bounds are published at `https://github.com/selloriybrendi/congruent-rank7-minimal` (archived on Zenodo). A single command (`verify_all.py`, `verify_yakun.py`) re-checks every claim; each checker was mutation-tested.

Use of generative AI

Claude Opus 5.5 (Anthropic) via Claude Code was used to write and run the programs and to help prepare the text, under the author's direction; every number in the paper was produced by the programs and re-checked. The author takes full responsibility.

References

[1] A. Dujella, A. S. Janfada, S. Salami, *A search for high rank congruent number elliptic curves*, J. Integer Seq. 12 (2009), Article 09.5.8, `https://cs.uwaterloo.ca/journals/JIS/VOL12/Janfada/janfada3.pdf`.

[2] P. Monsky, appendix to D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem, II*, Invent. Math. 118 (1994), 331–370, doi:10.1007/BF01231536.
[3] N. F. Rogers, *Rank computations for the congruent number elliptic curves*, Experiment. Math. 9 (2000), 591–594, doi:10.1080/10586458.2000.10504662; PhD thesis (2004).
[4] OEIS Foundation, A194687.
[5] The PARI Group, PARI/GP 2.17.4.
[6] J. E. Cremona, `mwrank` / eclib.