Rank of an elliptic curve and 3-rank of a quadratic field via the Burgess bounds

ANTS-16, July 2024 at MIT

Noam D. Elkies

Harvard University, Cambridge, MA USA

Overview

- Elliptic curves $E_k : y^2 = x^3 + k$ with $j = 0$ ("Mordell curves")

- A curve E_k of rank at least 16

- 3-isogeny descent to 3-torsion in quadratic class group;
E_k has rank 16 under GRH

- Burgess bound with Booker and Treviño's constants
$\Rightarrow$ E_k has rank 16 unconditionally

- Further records and challenges

Mordell curves. An elliptic curve $E/\mathbf{Q}$ has $j = 0 \iff$ $\mathrm{End}(E) = \mathbf{Z}[\boldsymbol{\mu}_3] \iff E$ can be written as the "Mordell curve"

$$E_k : y^2 = x^3 + k$$

for some $k \in \mathbf{Q}^\times$. Two such curves $E_k, E_{k'}$ are isomorphic $\iff$ $k'/k \in (\mathbf{Q}^\times)^6$, so we may assume $k \in \mathbf{Z}$ and k is 6th power free.

Mordell's theorem (1922, same year as Mordell's conjecture):

For any elliptic curve $E/\mathbf{Q}$, its set $E(\mathbf{Q})$ of rational points is an abelian group of finite torsion and rank.

In particular this is true for $E = E_k$.

So, what are the possible torsion groups $E_k(\mathbf{Q})_{\mathrm{tors}}$ and ranks?

Torsion in Mordell curves. As usual for such families, torsion is much easier than rank. The only possible torsion in $E_k(\mathbf{Q})$:

- a 2-torsion point $(-n, 0)$ if $k = n^3$
  [quadratic twist of $y^2 = x^3 + 1$];
- 3-torsion points $(0, \pm m)$ if $k = m^2$
  [cubic twists of E_1, which has both 2- and 3-torsion, so also 6-torsion: $(2, \pm 3)$];
- 3-torsion points $(12, \pm 36)$ on E_{-432}
  [Fermat cubic curve $X^3 + Y^3 + Z^3 = 0$].

Otherwise $E_k(\mathbf{Q})$ has trivial torsion.

[*Can you find* $k \in \mathbf{Q}(\boldsymbol{\mu}_3)^\times$ *for which* $E_k(\mathbf{Q}(\boldsymbol{\mu}_3))$ *has 7-torsion? Likewise 5-torsion on* $y^2 = x^3 + ax$ *(*$j = 1728$*, CM by* $\mathbf{Z}[i]$*) over* $\mathbf{Q}(i)$.]

Ranks of Mordell curves. The possible $\mathbf{Q}$-ranks of curves E_k are much harder to understand than the torsion. For now, large ranks are the topic of speculation and record-hunting, not theorems.

NDE on `nmbrthry`, 6 Feb. 2016: E_{16D} has rank ≥ 16 for

$$D = 7251383465384782853945032549 3 = 41p$$

where $p =$ the prime 176863011350848362291342257 3.

Proved by searching for points and finding a bunch that generate a rank-16 subgroup of $E_{16D}(\mathbf{Q})$. (See paper for a list of 16 independent points.)

Expect rank = 16 exactly. How hard could that be to prove?

\repeat{**How hard is it to <u>prove</u> we have the right rank?**}

Short of invoking BSD conj., all we know to do is compute Selmer groups (descent); how hard is that?

Comparison with other families:

E with $E_{\text{tors}} = T \neq \{0\}$ (e.g. a record $|T| = 2$ curve with $r = 20$ from [NDE–Klasgbrun, ANTS-14, 2020]): entirely feasible to compute Selmer groups for isogeny $\varphi : E \to E/T'$ (some nontrivial subgroup $T' \subseteq T$) and its dual $\hat{\varphi} : E/T' \to E$. For high-rank curves, the resulting rank bound usually matches the rank of the known subgroup of $E(\mathbf{Q})$, so we're done.

E unconstrained (e.g. the $r = 28$ curve of [NDE 2006]): need 2-torsion in class group of a large-disc. cubic extension $F/\mathbf{Q}$ with Galois closure $\mathbf{Q}(E[2])$. Needs GRH for all unram. abelian extensions of F, as in [Klagsbrun–Sherman–Weigandt 2019].

So how hard is it to prove we have the right rank of E_k?

Our curves $E_k : y^2 = x^3 + k$ are intermediate: not as easy as curves with nontrivial torsion T, nor as intractable as unconstrained curves.

As with $|T| > 1$ curves, we can use isogeny descents, here via a 3-isogeny $\varphi : E_k \to E_{-27k}$ and its dual (see next slide).

As with unconstrained curves, the Selmer group involves torsion in a class group, here 3-torsion in the class groups of the quadratic fields $\mathbf{Q}(\sqrt{k})$ and its "mirror field" $\mathbf{Q}(\sqrt{-3k})$. That's still more accessible than a noncyclic cubic extension of huge discriminant.

The 3-isogenies between E_k and E_{-27k}.

We can construct $\varphi : E_k \to E_{-27k}$ from the CM of E. Fix a cube root of unity ρ. Then $\mathrm{End}_{\bar{\mathbf{Q}}} E_k = \mathbf{Z}[\rho]$ with ρ acting by $(x, y) \mapsto (x, \rho y)$. Hence $\sqrt{-3} = \rho - \bar{\rho}$ is a 3-isogeny with kernel $\{\mathbf{0}, (0, \sqrt{k}), (0, -\sqrt{k})\}$, the points P s.t. $\rho P = \bar{\rho} P$.

This isogeny is defined only over the CM field $\mathbf{Q}(\rho) = \mathbf{Q}(\sqrt{-3})$, but with rational x and $y/\sqrt{-3}$. So, we get a 3-isogeny φ defined over $\mathbf{Q}$ from E_k to its quadratic twist by $\mathbf{Q}(\sqrt{-3})$, which is E_{-27k}. Explicitly,

$$\phi(x, y) = \left(\frac{x^3 + 4k}{x^2}, \frac{(x^3 - 8k)y}{x^3} \right).$$

The action of $\mathbf{Z}[\rho]$ on E_{-27k} then gives us $\widehat{\varphi}$, with kernel $\{\mathbf{0}, (0, \sqrt{-27k}), (0, -\sqrt{-27k})\}$.

[Yes, this generalizes to other CM curves.]

The φ- and $\widehat{\varphi}$-descents. Our D is $1 \bmod 4$, so the curves E_k and E_{-27k} (with $k = 16D$ as before) have good reduction at 2; e.g. E_k has model

$$x^3 = y^2 + y - \frac{D-1}{4} = \left(y + \frac{1+\sqrt{D}}{2}\right)\left(y + \frac{1-\sqrt{D}}{2}\right).$$

The factors $y + (1 \pm \sqrt{D})/2$ of x^3 are Weil functions. Choosing $+\sqrt{D}$, get homomorphism $\delta : E_{16D}(\mathbf{Q}) \to \mathbf{Q}(\sqrt{D})^\times/(\mathbf{Q}(\sqrt{D})^\times)^3$ taking (x, y) [other than $\mathbf{0}$ and $(0, -(1+\sqrt{D})/2)$] to the class of $y + (1+\sqrt{D})/2$, with $\ker(\delta) = \widehat{\varphi}(E_{-27k}(\mathbf{Q}))$.

This connects the Selmer group for $E_k(\mathbf{Q})/\widehat{\varphi}(E_{-27k}(\mathbf{Q}))$ with $H_D[3]$, where H_D is the class group of $\mathbf{Q}(\sqrt{D})$.

Likewise the Selmer group that contains $E_{-27k}(\mathbf{Q})/\varphi(E_k(\mathbf{Q}))$ involves $H_{-3D}[3]$.

The φ- and $\hat{\varphi}$-descents, cont'd.

Since D is squarefree (and also $1 \bmod 4$ but $\neq 1$), The only other contribution to the Selmer groups is U/U^3 where $U =$ unit group of $\mathbf{Q}(\sqrt{D})$. Therefore

$$r(E_k) \leq \dim_{\mathbf{Z}/3\mathbf{Z}} H_D[3] + \dim_{\mathbf{Z}/3\mathbf{Z}} H_{-3D}[3] + 1.$$

Using the known subgroup $\cong \mathbf{Z}^{16}$ of $E_k(\mathbf{Q})$ we find

$$\dim_{\mathbf{Z}/3\mathbf{Z}} H_D[3] \geq 7, \qquad \dim_{\mathbf{Z}/3\mathbf{Z}} H_{-3D}[3] \geq 8.$$

These are the current records for the 3-rank of a real and imaginary quadratic field respectively. Also, 3-rank 8 with $|3D| < 3^{61.5}$ compares favorably with the Cohen-Lenstra proportion of about 3^{-64}.

(This use of high $r(E_k)$ to find high 3-ranks is already in [Quer 1987], when the records were $12 = 5 + 6 + 1$.)

3-torsion in H_D and H_{-3D}. Since

$$r(E_k) \le \dim_{\mathbf{Z}/3\mathbf{Z}} H_D[3] + \dim_{\mathbf{Z}/3\mathbf{Z}} H_{-3D}[3] + 1,$$

$r(E_k) = 16$ would follow from

$$\dim_{\mathbf{Z}/3\mathbf{Z}} H_D[3] \stackrel{?}{=} 7, \qquad \dim_{\mathbf{Z}/3\mathbf{Z}} H_{-3D}[3] \stackrel{?}{=} 8,$$

and these two "$\stackrel{?}{=}$" are equivalent by the reflection theorem [Scholz 1932].

Magma soon computes

$$H_{-3D} \stackrel{\text{GRH}}{\cong} (\mathbf{Z}/2\mathbf{Z})^2 \times \boxed{(\mathbf{Z}/3\mathbf{Z})^8} \times (\mathbf{Z}/77681\mathbf{Z}) \times (\mathbf{Z}/139939\mathbf{Z}),$$

$$H_D \stackrel{\text{GRH}}{\cong} (\mathbf{Z}/2\mathbf{Z})^2 \times \boxed{(\mathbf{Z}/3\mathbf{Z})^7}.$$

What would it take to remove one of these GRH assumptions?

From $(H_{-3D})_0$ to H_{-3D}

Consider H_{-3D}, and denote by $(H_{-3D})_0$ the known subgroup $(\mathbf{Z}/2\mathbf{Z})^2 \times (\mathbf{Z}/3\mathbf{Z})^8 \times (\mathbf{Z}/77681\mathbf{Z}) \times (\mathbf{Z}/139939\mathbf{Z})$. Actually a known homomorphism from $(H_{-3D})_0$ to H_{-3D}, but we soon prove unconditionally that it's injective. It is surjectivity that's hard: how to prove we've found <u>all</u> of H_{-3D}?

Enough to prove $|H_{-3D}| = |(H_{-3D})_0|$.

By Legendre $|H_{-3D}|$ is a multiple of $|(H_{-3D})_0|$. Moreover, we have all of $H_{-3D}[2]$ by genus theory, and $H_{-3D}[4] = H_{-3D}[2]$ using [Rédei 1934], so $[H_{-3D} : (H_{-3D})_0]$ is odd.

Thus we need only show $|H_{-3D}| < 3\,|(H_{-3D})_0|$.

Bounding $|H_{-3D}|$. Dirichlet's class number formula gives

$$|H_{-3D}| = \frac{\sqrt{3D}}{\pi} L(1, \chi_{3D}) = \frac{\sqrt{3D}}{\pi} \sum_{n=1}^{\infty} \frac{\chi_{3D}(n)}{n}$$

where $\chi_{3D} = (\frac{-3D}{\cdot})$. So we expect $L(1, \chi_{3D}) = 1.921597\ldots$ and need only show $L(1, \chi_{3D}) < 5.764$.

It's easy enough to numerically compute $\sum_{n=1}^{N} \chi_{3D}(n)/n$ for N large enough to get quite close to $1.921597\ldots$. But how to prove that the remainder

$$R(\chi_{3D}, N) := \sum_{n=N+1}^{\infty} \frac{\chi_{3D}(n)}{n}$$

is less than about 3.8?

Bounding $R(\chi_{3D}, N)$.

Start by writing $R(\chi_{3D}, N) := \sum_{n>N}^{\infty} \chi_{3D}(n)/n$ in terms of

$$S(x) := \sum_{1 \le n \le x} \chi_{3D}(n)$$

via "partial summation" / integration by parts:

$$\int_{N+\frac{1}{2}}^{\infty} \frac{1}{x}\, d(S(x) - S(N)) = \int_{N+\frac{1}{2}}^{\infty} (S(x) - S(N))\, \frac{dx}{x^2}\,.$$

Now $|S(x) - S(N)| \le x - N$ (because each $|\chi_{3D}(n)| \le 1$); and $S(x) - S(N) \ll \sqrt{3D} \log 3D$ (Pólya–Vinogradov 1918, with small $\ll$-constant). So, enough to take $N \ll D^{1/2} \log D$, as usual for unconditional computations of class groups etc. But for our $D \sim 7 \cdot 10^{28}$ that's $N \sim 10^{16}$ — not happening (at least not anytime soon).

The Burgess bound.

We expect $S(x) - S(N) \ll (x - N)^{1/2+o(1)}$ once $x - N \ll q^\eta$ (any $\eta > 0$), but nothing like that is known unconditionally.

But we could use any improvement over trivial $|S(x) - S(N)| \le x - N$ with $x - N$ significantly smaller than $D^{1/2}$ . . .

Burgess (1962) supplied such a bound on short character sums

$$S_\chi(N, H) := S(N + H) - S(N) = \sum_{h=1}^{H} \chi(N + h)$$

for nontrivial characters χ of prime modulus p:

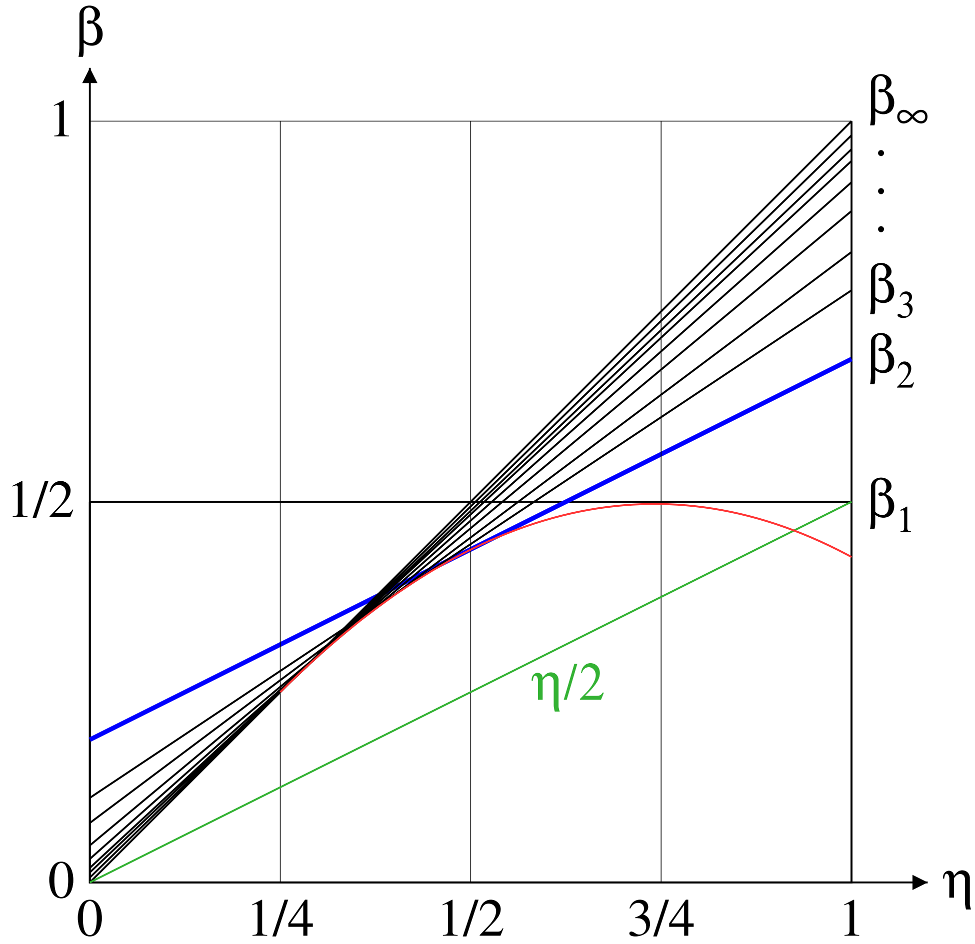
$$S_\chi(N, H) \ll_r (\log p)^{1/r} H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}}$$

for each $r = 2, 3, 4, \ldots$. Thus $\eta > 1/4 \Longrightarrow S_\chi(N, p^\eta) = o(p^\eta)$:

If $H = p^\eta$ then $S_\chi(N,H) \ll_r (\log p)^{1/r} H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}}$ yields

$$S_\chi(N,H) \ll p^{\beta_r + o(1)} \quad \text{where} \quad \beta_r = \left(1 - \frac{1}{r}\right)\eta + \frac{r+1}{4r^2}.$$

Plot of $\beta_1 = 1/2$, $\boxed{\beta_2 = \eta/2 + 3/16}$, $\beta_3 = 2\eta/3 + 1/9$, $\ldots$, $\beta_\infty = \eta$:



Burgess is better than Pólya–Vinogradov (i.e. $\beta_r < 1/2$) for $\eta < (2r+1)/4r$, and better than trivial (i.e. $\beta_r < \eta$) for $\eta > (r+1)/4r$. These are 5/8 and 3/8 for $r = 2$.

The modulus $3D$ of χ_{3D} is not quite prime, but $3D = 123p$. We split the sum into $\phi(123) = 80$ AP's, each of which is $\pm S_\chi(N', H/123)$ for $\chi = (\cdot/p)$, and apply Burgess to each S_χ.

The upper bound on $|R(\chi_{3D}, N)|$ is $\ll (\log p)^{1/2} p^{3/16} N^{-1/2}$, so we need $N \gg p^{3/8+o(1)}$. The $p^{1/8}$ saving is enough to make this practical — provided the $\ll$-constant is small enough to make the $\gg$-constant tolerable!

So what are these constants?

Burgess's proof is entirely effective (clever use of Weil's bounds on complete character sums) but rather complicated . . .

The Burgess–Booker–Treviño bounds.

Fortunately Booker (2006) already worked out numerical bounds in a very similar context. For $r = 2$,

$$|S_\chi(N,H)| \le 1.8221\, p^{3/16}(\log p + 8.9077)^{1/4} H^{1/2}$$

once $p > 10^{20}$ (which our p is, $> 1.7 \cdot 10^{27}$).

This requires $H < 2\sqrt{p}$. Booker used a better (but slower to compute) approximation to $L(1,\chi)$ than just a partial sum so that the remainder involves only $H < 2\sqrt{p}$. We fill in $H > 2\sqrt{p}$ using the weaker but uniform bound from Treviño (2015):

$$|S_\chi(N,H)| \le 2.74\, p^{3/16}(\log p)^{1/2} H^{1/2}$$

for any $p > 10^7$ and all N, H. We conclude that

$$|R(\chi_{3D}, N)| < \frac{8 \cdot 10^6}{\sqrt{N}} + 0.4\,.$$

Computational conclusion.

We took $N = 2^{43} < 10^{13}$; this makes $|R(\chi_{3D}, N)| < 3.1$.

We computed $\sum_{n=1}^{N} \chi_{3D}(n)/n$ numerically twice: first in floating point (large n to small), then as $2^{-61} \sum_{n=1}^{N} \chi_{3D}(n) \lfloor 2^{61}/n \rfloor$ summing in 64-bit integer arithmetic. Either way it took < 24 hours on 16 processors, and the sum is within 10^{-6} of the expected value $1.92\ldots$ of $L(1, \chi)$.

Combining everything we find that $[H_{-3D} : (H_{-3D})_0] < 3$; since that index is known to be odd, it equals 1 and we are done. $\square$

Further records and challenges.

As $\widehat{\varphi}$- and φ-descents related $r(E_k)$ to $H_k[3]$ and $H_{-3k}[3]$, a 2-descent relates $r(E_k)$ to the 2-rank of the "pure cubic field" $\mathbf{Q}(k^{1/3})$. We thus get the current record of ≥ 15 for this 2-rank, but here we prove rank exactly 15 only under GRH.

Our E_{16D} and E_{-432D} are not the highest-rank Mordell curves known: E_k and E_{-27k} have rank at least 17 for

$$\begin{aligned} k &= -908800736629952526116772283648363 \\ &= -2195745961 \cdot 413891567044514092637683. \end{aligned}$$

[The relevant 3-ranks are still 7 and 8 due to bad reduction at 2; likewise no new 2-rank record for $\mathbf{Q}(k^{1/3})$.] Rank equals 17 under GRH, but not unconditionally while Burgess is limited to prime (and nearly-prime) moduli. It's been 60+ years since [Burgess 1962]. . .

$\mathcal{THE\ \ END}$

$\mathcal{THANK\ \ YOU}$

P.S. The $j = 1728$ curve $y^2 = x^3 - (1 + 2i)x$ has 5-torsion at $(x, y) = (1, 1 - i)$ [in $\ker(2 - i)$];

The $j = 0$ curve $y^2 = x^3 - 6^4(5 + \rho)$ has 7-torsion at $(x, y) = (12(1 + 2\rho), 108\rho)$ [in $\ker(2 - \rho)$].