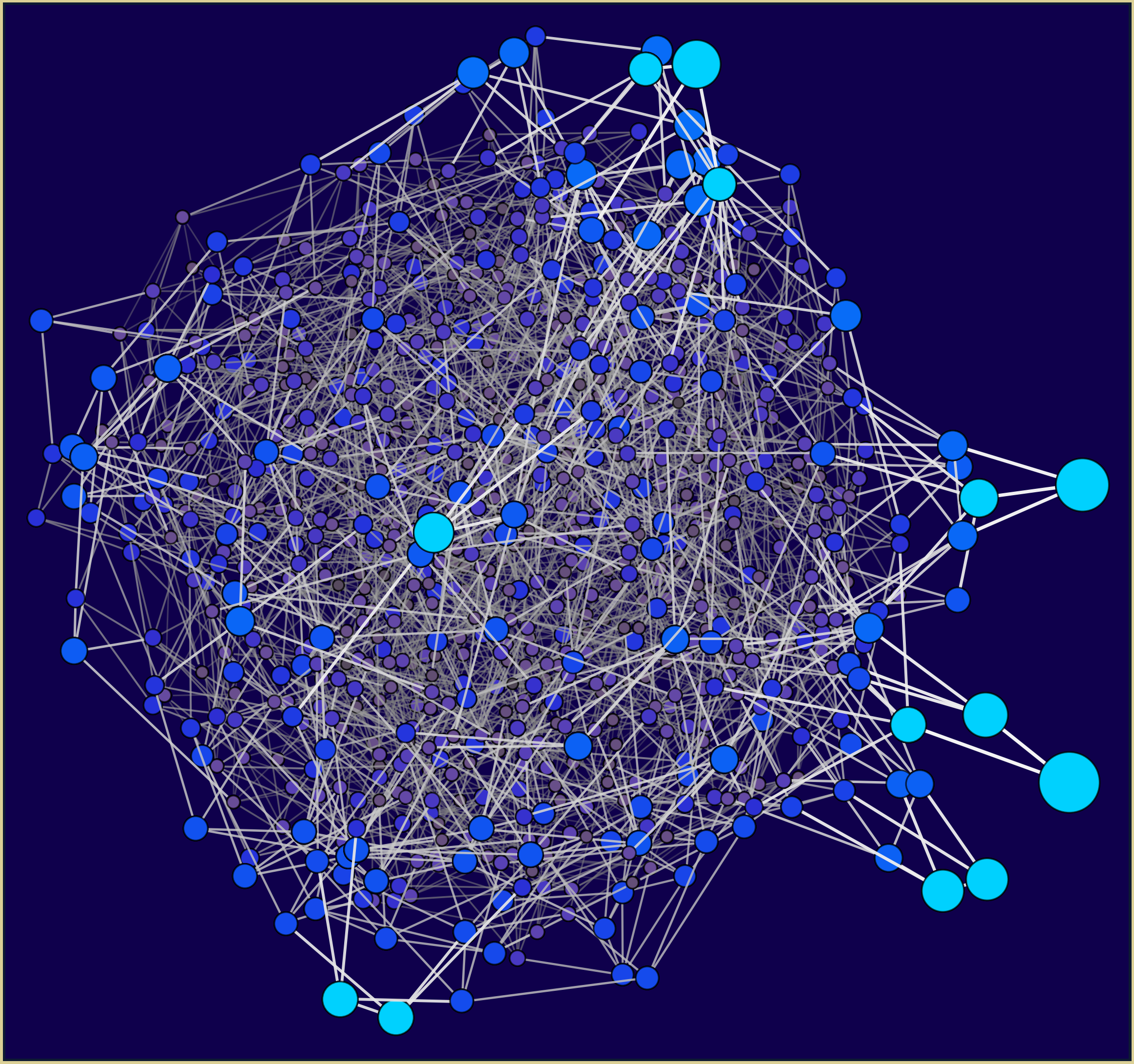
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth
Algorithmic Number Theory Symposium

New rank records for elliptic curves having rational torsion

Noam D. Elkies and Zev Klagsbrun



msp

THE OPEN BOOK SERIES 4 (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.233

New rank records for elliptic curves having rational torsion

Noam D. Elkies and Zev Klagsbrun

We present rank-record breaking elliptic curves having torsion subgroups $\mathbb{Z}/n\mathbb{Z}$ for $n = 2, 3, 4, 5, 6$, and 7.

1. Introduction

Given an elliptic curve $E/\mathbb{Q}$, the Mordell–Weil theorem states that the group of rational points $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}^r \times T$, where r is the *rank* of E and T is a finite group called the *torsion subgroup* of E [21]. While the groups that can appear as T were fully characterized by Mazur [16], which ranks occur is a question that goes back to Poincaré [26] and has been the subject of competing folklore conjectures.

One side, claiming ranks are bounded, was recently bolstered by several different models [30; 31; 25] that predict that all but finitely many elliptic curves have rank at most 21, with stronger conjectured bounds on which ranks occur infinitely often for each possible torsion group T. (For example, if $T = \mathbb{Z}/n\mathbb{Z}$ for $n = 2, 3, \ldots, 8$ then the bound 21 is replaced by 13, 9, 7, 5, 5, 3, 3.) The other side, arguing that ranks are unbounded, has relied on periodically exhibiting curves of larger and larger rank.

Our work continues that tradition, exhibiting rank-record breaking curves for the torsion subgroups $\mathbb{Z}/n\mathbb{Z}$ for each $n = 2, 3, 4, 5, 6, 7$, which constitute two-fifths of the 15 groups that Mazur showed can appear as the torsion subgroup of an elliptic curve over $\mathbb{Q}$.

At the same time, our work provides, at best, limited evidence that ranks are unbounded. We broke six different records, and found numerous new curves whose ranks tie the old records (and many more whose ranks exceed the heuristically conjectured asymptotic upper bounds). But the scale of this search was vastly larger than any previously attempted, and yet we could not break any of the previous records by more than 1, and in each case found only a handful of curves (in most cases, a single curve) with the new record rank. This suggests that the growth of ranks of elliptic curves might indeed peter out at some point.

Elkies was supported by NSF grants DMS-0501029, DMS-1100511, and DMS-1502161, a Radcliffe Fellowship, and the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation.
MSC2020: 11G05.
Keywords: elliptic curves, ranks of elliptic curves.

1.1. ***Organization.*** This paper largely splits into three parts. The first consists of Sections 2–6, which describe the methods that we used to search for curves of high rank, as well as Section 7, which presents some open questions about our methods. The second, Sections 8–14, describes our results, including details of our searches in each of the torsion families considered. Section 9 also includes a previously unpublished family of elliptic K3 surfaces $\mathcal{E}_u/\mathbb{Q}(t)$ that have Mordell–Weil group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^9$ for each $u \neq \pm 1, \pm 2$ for which $5 - u^2$ is a square. We exhibit generators for $\mathcal{E}_u(\mathbb{Q}(t))$ in Appendix A. The third and final part of this paper is Appendix B, which presents models for the record-breaking curves we discovered and points that generate their Mordell–Weil groups.

2. The method of Mestre and Nagao

The core ingredient in our search was a well-known method, originally from Mestre, to find elliptic curves having large Mordell–Weil rank. We start with an elliptic fibration $\mathcal{E}/\mathbb{Q}(t)$ having Mordell–Weil rank r, and then attempt to find good values of t for which the specialization E_t has particularly large rank [20].

A theorem of Silverman [27] states that all but finitely many specializations E_t of $\mathcal{E}$ have rank at least r, so this approach effectively gives us r independent rational points on each specialization for free.

The method for finding values of t for which the rank of E_t is significantly larger than r has its roots in the observation of Birch and Swinnerton-Dyer that curves that have unusually many points modulo p for most p should have many rational points as well [3], and in Mestre's work on Weil's explicit formula for elliptic curves [18]. The idea is to construct a score $S(t, B)$ that incorporates the number of points $N_p(E_t)$ on $\overline{E}_t(\mathbb{F}_p)$ for all primes $p \le B$ where E_t has good reduction, and then to search for rational points on E_t for those values of t in a search region for which $S(t, B)$ is above some threshold. While this basic method was first used by Mestre to find the first curves over $\mathbb{Q}$ having rank 12 [17], its first use in a family $\mathcal{E}/\mathbb{Q}(t)$ appears to be due to Nagao [23].

Nagao considered the scores

$$S_1(t, B) = \sum_{\substack{p<B,\\ E_t \text{ has good reduction at } p}} \frac{-a_p(E_t)+2}{N_p(E_t)} \log p \quad \text{and} \quad S_2(t, B) = \frac{1}{B} \sum_{\substack{p<B,\\ E_t \text{ has good reduction at } p}} -a_p(E_t) \log p,$$

which, when large, suggest via Weil's explicit formula for elliptic curves [18] that the order of the vanishing of the L-function $L_{E_t}(s)$ at $s = 1$ should be large as well.

We choose to evaluate a different sum,

$$S(t, B) = \sum_{\substack{p<B,\\ E_t \text{ has good reduction at } p}} \log\left(\frac{N_p(E_t)}{p}\right), \tag{1}$$

as in [8], so that $\exp(-S(t, B))$ is the partial product

$$\prod_{\substack{p<B,\\ E_t \text{ has good reduction at } p}} (1 - a_p(E_t)p^{-s} + p^{1-2s})^{-1} \tag{2}$$

of the Euler product for $L_{E_t}(s)$ evaluated at $s = 1$ (ignoring the finitely many factors at primes of bad reduction). The conjecture of Birch and Swinnerton-Dyer suggests that when E_t has large rank such partial products should rapidly approach zero, and thus that $S(t, B)$ should be large.

3. Computational techniques

Computing any of the sums in Section 2 would be computationally infeasible for a large range of t if one needed to individually compute $a_p(E_t)$ for each $p < B$ and each value of t. To scale Mestre's method to extremely large search regions, we took advantage of three computational tricks.

First, as observed by Nagao [24], $a_p(t)$ depends only on $t \pmod p$. As a result, one can first compute $a_p(t)$ for all $p \le B$ and for all $t \in \mathbb{F}_p$ for which $\Delta_{E_t} \ne 0$, and then use the precomputed values to calculate $S(t, B)$ for each t in the search region.

The second trick, also due to Nagao [24], lets us concentrate our computation on the most promising values of t. Rather than compute $S(t, B)$ for all t in the search region, we choose an increasing series of bounds $B_0 \le B_1 \le \cdots \le B_m = B$ and cutoffs $C_0 \le C_1 \le \cdots \le C_m = C$, and only compute $S(t, B_i)$ for $i \ge 1$ for those values of t for which $S(t, B_j) \ge C_j$ for all $0 \le j < i$.

These first two tricks appear to be well known (see [12], for example). The third trick, which is apparently due to Elkies [8], seems to be less widely known, and we describe it in detail below.

3.1. ***Sieving.*** Rather than computing $S(t, B)$ for each value of t by looking up the values of $N_p(t)$ (or more likely, $\log(N_p(t)/p)$) for each prime $p < B$, sieving computes $S(t, B)$ for a large number of values of $t = a/b$ at once. The algorithm works as follows:

Fix a value of b and an interval $[a_0, a_0 + N)$. We allocate a counter array $\mathcal{C}$ of length N initialized to zero. For each prime $p \nmid b$, we initialize an update array $\mathcal{P}$ of length p such that the i-th entry of $\mathcal{P}$ is equal to $\log(N_p(b^{-1}(a_0 + i))/p)$. We then repeatedly add the update array $\mathcal{P}$ into $\mathcal{C}$, starting with position zero in $\mathcal{C}$ and shifting the starting position by p with each iteration. Doing this for each prime $p \le B$ tallies the sum $S(t, B)$ into the counter array $\mathcal{C}$ for all $t = a/b$ with $a_0 \le a < a_0 + N$.

By loading $\mathcal{P}$ nonsequentially, we can read the values of $\log(N_p(b^{-1}(a_0 + i))/p)$ sequentially from memory, while requiring only a single inversion modulo p and no additional multiplications, divisions, or modular reductions.

To avoid the cost of floating point operations, we do not store $\log(N_p(t)/p)$ as a floating-point number, but round it to a rational number with fixed denominator D and store the numerator $\lfloor D \log(N_p(t)/p) + \frac{1}{2} \rfloor$. The sieve then tallies these numerators for each t using integer addition, which is faster than floating-point arithmetic. The common denominator D should be large enough that rounding errors do not appreciably degrade the score, but small enough that we can keep a large counter array in the high-speed cache. We found that by taking $D = 1024$, we were able to fit all of our scores into 16-bit integers.

We further took advantage of a feature of modern processors known as vector instructions. These are processor level instructions that can be used to perform the same operation on multiple consecutive elements of an array simultaneously. This allowed us to add 16 elements from the update array $\mathcal{P}$ into the counter array $\mathcal{C}$ at once, rather than one at a time.

Compared with computing each $S(t, B)$ individually, sieving is extremely fast. For example, for a fixed value of b, we are able to compute $S(a/b, 2^{16})$ for 2^{20} values of a in 3.2 seconds on a single thread of a hyperthreaded 2.3 GHz Intel Skylake Xeon processor. Smaller values of B take even less time; for example, computing $S(a/b, 2^{13})$ for 2^{20} values of a takes only 0.19 seconds on the same processor.

The large speed-up offered by this sieve-like technique is available only in the first step of Nagao's second trick described above: we can use it to quickly compute $S(t, B_0)$ for all t in the search region, but not to compute $S(t, B_i)$ for $i \geq 1$ on a restricted set of t. For $i \geq 1$ we must look up individual values of $\log(N_p(t)/p)$. However, because the sieve-like technique is so efficient, we can set B_0 large enough that computing $S(t, B_0)$ is the dominant portion of the work — see Section 6.

4. Choosing fibrations

Perhaps the most important ingredient in searching for high-rank elliptic curves is choosing a good fibration to search on. We'll describe the factors that guided our choices, while leaving the specific choices of fibrations to Sections 9 — 14.

In the past, the largest rank elliptic curves having torsion subgroups $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, and $\mathbb{Z}/4\mathbb{Z}$ have come from specializations of K3 surfaces having relatively large rank (9 for $\mathbb{Z}/2\mathbb{Z}$, 5 for $\mathbb{Z}/3\mathbb{Z}$, and 4 for $\mathbb{Z}/4\mathbb{Z}$). Our search was no different, focusing on the same families in which the previous records were found.

By contrast, high-rank K3 surfaces are not known to exist for the other torsion groups we considered. The largest known rank of a K3 surface having torsion subgroup $\mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$ is 1, and the universal elliptic curve having a point of order 7 is already a K3 surface, of generic rank zero. As a result, previous searches have focused on high-degree elliptic surfaces of larger rank [15; 6].

We initially attempted to do the same for the group $\mathbb{Z}/6\mathbb{Z}$ using a degree 4 elliptic surface of Kihara having rank 3 [14] considered in [6]. We found that while this surface has a relatively large number of low-height rank 8 specializations, we could not find any such specializations of parameter height larger than $\approx 2^{13.5}$. This suggested that as the height of t grew, either the number of high-rank specializations in this family decayed rapidly or our scores quickly became less meaningful.

While [6] considered other degree 4 elliptic surfaces having Mordell–Weil group $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}^3$, we concluded that the low-hanging fruit on these had already been discovered, and that our best hope of finding a rank 9 curve having torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ was to search on the universal elliptic curve with a point of order 6, which is a rational surface. We made a similar decision regarding the groups $\mathbb{Z}/n\mathbb{Z}$ for $n = 5$ and $n = 7$, for which the universal elliptic curve over $\mathrm{X}_1(N)$ is respectively rational and K3.

Remark. Subsequent to ANTS-XIV but prior to publication, Maksym Voznyy discovered a rank 9 curve with torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ as a low-height specialization of an elliptic surface of degree 4 having Mordell–Weil group $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}^2$ [29]. This curve is somewhat larger than the one we present in Section 13, and appears in [5].

5. Computing ranks

After finding a set of values of t such that $S(t, B)$ is sufficiently large, we are left with the problem of identifying those that actually have large rank. We approach this problem in two stages. First, we use descent methods to obtain an upper bound on the rank. For those specializations where the upper bound is sufficiently large, we then search for points on whichever coverings we can efficiently compute.

5.1. ***Descent computations.*** For half of the families we considered, the torsion subgroup contains a point of order 2, so we could use Fisher's machinery for computing rank bounds using 2-power isogeny Selmer groups, available in Magma via the command `TwoPowerIsogenyDescentRankBound` [13]. For all of the specializations we considered where this upper bound was at least as large as the previous record in the family, the upper bound was in fact equal to the rank (though of course we did not know this until after we searched for points).

For the specializations with torsion subgroup $\mathbb{Z}/3\mathbb{Z}$, there is no 2-isogeny over $\mathbb{Q}$, and a full 2-descent was out of reach. This forced us to consider a different approach.

As a first attempt, we ran all of the high scorers through a slightly modified version of Magma's `ThreeIsogenySelmerGroups` command to obtain a coarse rank bound. While the rank bound coming from 3-descent via isogeny tends to be reasonably tight for small curves, many of the specializations we considered had a large number of places of split multiplicative reduction, which boosted this bound for structural reasons unconnected to rank. To deal with this, we then used our own implementation of the algorithm for computing the Cassels–Tate pairing developed by Fisher and van Beek [1; 2] to compute the 3-Selmer rank of each specialization for which the rank bound coming from 3-isogeny descent was at least 14.

For the curves with $\mathbb{Z}/5\mathbb{Z}$ torsion, we were able to use a modified version of the `pIsogenyDescent` command in Magma to compute a rank bound coming from 5-descent via isogeny, which allowed us to eliminate close to 99% of the candidate specializations. Since the fibration with $\mathbb{Z}/5\mathbb{Z}$ torsion that we searched is a rational surface over $\mathbb{Q}(t)$, the remaining specializations were sufficiently small that we could use Magma's built-in implementations for computing both the 2-Selmer group and the Cassels–Tate pairings for each one.

The curves with $\mathbb{Z}/7\mathbb{Z}$ torsion posed a unique challenge. While we were able to use our modified version of Magma's `pIsogenyDescent` command to compute a rank bound coming from 7-descent via isogeny, this bound tended to be insufficiently sharp for our candidate specializations.

In addition, because the $\mathbb{Z}/7\mathbb{Z}$ fibration we considered is a K3 surface over $\mathbb{Q}(t)$, we expected that the size of our specializations would overwhelm Magma's 2-descent machinery. However, we discovered that while the discriminant of this surface has degree 24, the discriminant of the cubic subfield of its 2-division field has degree only 6. As a result, although the curves in question were quite large, it was still possible to perform 2-descent and the Cassels–Tate pairings on them.

5.2. ***Searching for points.*** Once we had candidate curves that our Selmer computations suggested had large rank, we needed to find enough independent points on them to verify that they had the expected rank.

Our main method for finding these points was by searching for points on 2-coverings of each curve using Magma's built-in functionality. For most of the groups — $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, and $\mathbb{Z}/7\mathbb{Z}$ — we were able to compute the complete 2-Selmer group for each of the curves in question.

For the group $\mathbb{Z}/2\mathbb{Z}$, we did the next best thing, computing the coverings corresponding to the elements of the Selmer group of a 2-isogeny and its dual, and searching on those.

In principle, we could have done something similar with the 3-isogeny coverings for the curves having torsion subgroup $\mathbb{Z}/3\mathbb{Z}$ using Elkies's lattice-based method of searching for points on cubic curves in $\mathbb{P}^2$ [7]. However, due to a memory leak we discovered[1] in Magma's implementation of Elkies's method, doing so would have required additional effort. Instead, we searched the 2-coverings corresponding to the known points on each curve coming from the rational points on the surface $\mathcal{E}$, adding new 2-coverings to the mix whenever we discovered an additional point.

Somewhat surprisingly, this method worked extremely well. We suspect that because each of the curves in question has a large number of points of low height, we likely would have found them using nearly any method we attempted.

6. Choosing parameters

There is an art to choosing proper values for B_i and C_i. The goal, of course, is to minimize the total time spent searching, while not missing any of the top candidates. How to do this is unclear. We chose our values experimentally, and we suspect that our choices were far from optimal; see Section 7. Some tradeoffs however are straightforward.

If C_0 is too small, then too many values of t pass the initial cutoff, so the cost of computing $S(t, B_i)$ for $i \geq 1$ dominates, because looking up the values of $\log(N_p(t)/p)$ individually is far more expensive than sieving. Conversely, if C_0 is too large then we risk eliminating promising values of t.

We compromised by choosing C_0 rather aggressively, targeting a cutdown on the order of 10^3, but using a large enough value of B_0 (between 2^{13} and 2^{16}) to limit the risk of losing any good candidate t. (Previous searches have tended to take $B < 10^3$, so this seemed sufficiently conservative.)

The values of B_i for $i \geq 1$ are less important. We chose the B_i to be successive powers of 2 up to $B = 2^{18}$. We also chose our C_i less aggressively for $i \geq 1$, since these have a smaller effect on the runtime.

6.1. ***Skewed search regions.*** For some of the fibrations we considered, the polynomials defining the nontrivial coefficients of $\mathcal{E}$ were skew in the sense of [22]. Very roughly, this means that the higher degree coefficients tend to have larger magnitude than the smaller ones or vice versa.

As a result, the average magnitude of the coefficients of an integral model for E_t on a skewed search region (that is, $t = a/b$ with $\mathrm{Max}(|a|) = s\mathrm{Max}(|b|)$ for some $s \in \mathbb{Q}$) will be smaller than the average magnitude of the coefficients of an integral model for E_t on a square search region having the same size. While we don't have a firm grasp on how the existence of high-rank specializations is related to the

[1] While we discovered the presence of this memory leak, we did not attempt to identify its source.

coefficient size of E_t, it seems sensible to search for smaller curves, so we skewed our search regions accordingly.

7. Open questions

Although our search was largely successful, we are left with some open questions regarding the method of Mestre and Nagao.

(1) How large a prime bound should we be using relative to the search region/degree of the family?

Our experience indicates that the score $S(t, B)$ tends to be a poorer indicator of rank as the size of the search region grows, and that the rate at which it becomes less useful depends on the degree of the surface and on its torsion subgroup.

This is unsurprising, since we expect the convergence rate of the Euler product for $L_{E_t}(s)$ to depend on the conductor, which in turn grows roughly as a power of the height $H(t)$ depending on the degree and fiber types of the surface. (More precisely, the conductor is bounded above by a multiple of that power of $H(t)$, and for typical t this is the correct growth order.) We should therefore expect that we need to allow our prime bound B to grow as a function of $\mathcal{E}$ and $H(t)$ in order for $S(t, B)$ to remain useful. Is it possible to make this relationship precise?

(2) How can we incorporate the Tamagawa factors at the places where E_t has bad reduction?

It has been observed that the known curves of high rank tend to have split multiplicative reduction and large Tamagawa numbers at many small primes. While the L-function includes terms for the bad primes and these can be incorporated into $S(t, B)$, these terms don't incorporate the Tamagawa numbers.

One idea would be to include these primes into the score via the term $\log(c_p(E_t)(p-1)/p)$. However, this seems odd, because for surfaces with an isogeny, the Tamagawa numbers of E_t and its isogenous curves will generally not be the same, and any score that hopes to predict the rank should be isogeny-invariant.

In our searches, we found that including the term $\log(c(p-1)/p)$ with various c between 1 and 2 in $S(t, B)$ at each prime of split multiplicative reduction (effectively giving the specialization a fixed bonus for each such prime) tended to work reasonably well. At the same time, this is clearly a hack, and it would be nice to understand what the correct thing to do is.

(3) How closely should the rank be expected to correlate with $S(t, B)$?

One problem that we struggled with was understanding exactly how the score $S(t, B)$ should relate to the rank of E_t. For now, we are forced to choose our bounds conservatively to avoid missing any high-rank curves, which results in an increased amount of work, particularly at the descent steps.

Ideally, we would have a Bayesian score $\operatorname{Prob}(E_t \text{ has rank at least } r \mid S(t, B) > C)$ that would let us set the bounds B_i and C_i optimally, and inform our decision about how many curves to apply descent methods to. (The use of a Bayesian score was suggested to us by Joel Rosenberg.) Such a score would also let us estimate the likelihood that we missed a curve of high rank.

torsion subgroup	previous record	current record
$\mathbb{Z}/2\mathbb{Z}$	19	20
$\mathbb{Z}/3\mathbb{Z}$	14	15
$\mathbb{Z}/4\mathbb{Z}$	12	13
$\mathbb{Z}/5\mathbb{Z}$	8	9
$\mathbb{Z}/6\mathbb{Z}$	8	9
$\mathbb{Z}/7\mathbb{Z}$	5	6

Table 1. Rank records for various torsion subgroups.

8. Main results

We obtained new rank records for elliptic curves with torsion subgroups $\mathbb{Z}/n\mathbb{Z}$ for $n = 2, 3, 4, 5, 6$, and 7.

The current and previous records (as given by [5]) for each of these torsion subgroups are given in Table 1. We note that for the torsion subgroups $\mathbb{Z}/n\mathbb{Z}$ with $n = 2, 3, 4, 5, 6$, the ranks of both our curves and the previous record-holding curves are known unconditionally. While the ranks of some of the previous record-holding curves for the torsion subgroup $\mathbb{Z}/7\mathbb{Z}$ are known unconditionally, the ranks of our record holding curve as well as some of the previous record-holding curves are known only subject to the generalized Riemann hypothesis (GRH) for L-functions of number fields.

The next sections describe in greater detail the searches we carried out in pursuit of these records.

9. Curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z}$

For torsion groups $T = \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z}$ we proceeded as in [8], computing an elliptic fibration $\mathcal{E}(\mathbb{Q}_t)$ of a K3 surface X whose Néron–Severi group $\mathrm{NS}(X)$ is defined over $\mathbb{Q}$ and has high rank and large discriminant. For $T = \mathbb{Z}/3\mathbb{Z}$ and $T = \mathbb{Z}/4\mathbb{Z}$ we used the surface with $\mathrm{NS}(X)$ of rank 20 and discriminant -163. But for $T = \mathbb{Z}/2\mathbb{Z}$ this discriminant is not large enough; it turns out [10] that the highest rank attained by an elliptic fibration of X with a 2-torsion point is 8. Instead we use X with $\mathrm{NS}(X)$ of rank 19 but larger discriminant, which can attain Mordell–Weil rank 9.

Such X are parametrized by elliptic or Shimura modular curves, call them C, of level $\frac{1}{2}|\mathrm{disc}\,\mathrm{NS}(X)|$. When $|\mathrm{disc}\,\mathrm{NS}(X)|$ is large enough to allow Mordell–Weil rank 9, the curve C usually has genus at least 2, with few if any rational points (other than cusps and CM points, at which X or the elliptic fibration degenerates). In [8, pp. 8–9] Elkies reports using the sporadic rational point on the genus-2 curve $\mathrm{X}_0(191)/w$ to find such an X. A few years later he found a genus-zero Shimura curve of level 230 that could be used instead, giving a family of elliptic surfaces with Mordell–Weil group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^9$. Here $C = \mathcal{X}/w_{230}$, with $\mathcal{X}$ associated to the congruence subgroup $\Gamma_0(23)$ of the quaternion algebra ramified at $\{2, 5\}$. The family of surfaces with their elliptic fibrations was computed as in [9; 11]. The elliptic fibration is of the form $\mathcal{E}_u/\mathbb{Q}(t) : y^2 = x^3 + 2Ax^2 + Bx$, where

$$\begin{aligned} A = {} & (u^8 - 18u^6 + 163u^4 - 1152u^2 + 4096)t^4 + (3u^7 - 35u^5 - 120u^3 + 1536u)t^3 \\ & + (u^8 - 13u^6 + 32u^4 - 152u^2 + 1536)t^2 + (u^7 + 3u^5 - 156u^3 + 672u)t \\ & + (3u^6 - 33u^4 + 112u^2 - 80), \end{aligned} \tag{3}$$

and $B = \prod_{i=1}^{8} B_i(t, u)$ where

$$\begin{aligned} B_1(t, u) &= (u^2 + u - 8)t + (-u + 2), & B_3(t, u) &= (u^2 - u - 8)t + (u^2 + u - 10), \\ B_5(t, u) &= (u^2 - 7u + 8)t + (-u^2 + u + 2), & B_7(t, u) &= (u^2 + 5u + 8)t + (u^2 + 3u + 2), \end{aligned} \tag{4}$$

and $B_i(t, u) = -B_{i-1}(-t, -u)$ for $i = 2, 4, 6, 8$. Thus $\mathcal{E}_u \cong \mathcal{E}_{-u}$. If $5 - u^2$ is a square, and $u \neq \pm 1, \pm 2$ (to exclude CM points), then $\mathcal{E}_u$ has Mordell–Weil group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^9$ over $\mathbb{Q}(t)$. Generators are exhibited in Appendix A.

We searched for high-rank specializations of $\mathcal{E}_u$ for several values of u.

For $u = 2/5$, we searched the region $t = a/b$ with $0 < a < 2^{21}$ and $-2^{23} < b < 2^{23}$, finding 17 curves of rank 19, including the previous record-holding curve of Elkies that appears in [5], which occurs at $t = 11860/97527$.

For $u = 11/5$, we first applied the linear fractional transformation $t \mapsto (2 - t)/(t - 6)$ to $\mathcal{E}_u$ and then searched the region $t = a/b$ with $0 < a < 3 \cdot 2^{21}$ and $-2^{21} < b < 2^{21}$. We found one specialization of rank 20 at $t = -68559/32629$ ($t = -721141/2026305$ on the original model of $\mathcal{E}_u$), as well as another 20 specializations of rank 19, including one at $t = 100782/104143$ ($t = -26876/131019$ on the original model of $\mathcal{E}_u$) with smaller discriminant than the rank 19 curve of Elkies appearing in [5].

Minimal models and x-coordinates of a set of generators for the rank 20 specialization and the smallest discriminant rank 19 specialization appear in Appendix B.2. We note that this curve of rank 20 is the elliptic curve of largest rank for which the rank is known unconditionally.

We also searched regions of size roughly 2^{44} on each of the fibrations coming from $u = 2/13$ and $u = 22/13$, but did not find any specializations of rank greater than 18.

10. Curves with torsion subgroup $\mathbb{Z}/3\mathbb{Z}$

The singular K3 surface of discriminant -163 has (up to isomorphism) 159 elliptic fibrations with torsion group $\mathbb{Z}/3\mathbb{Z}$; their Mordell–Weil ranks range from 1 to 5. Rank 5 is attained by 13 of those fibrations, each giving rise to a family of elliptic curves whose Mordell–Weil group contains $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}^5$; the explicit formula will appear in [10].

We searched an appropriately skewed region of size 2^{43} on each of the 13 fibrations, finding 34 specializations of rank 14 (at least one on 11 of the 13 fibrations) as well as a single specialization of rank 15, given by

$$E : y^2 + 490738465519xy - 43280272918018887803567052242355787 5y = x^3.$$

Among the specializations having rank 14, the one with smallest conductor and discriminant is given by

$$E : y^2 + 6244332976xy + 220442125064192217455663037 5y = x^3,$$

which has smaller conductor and discriminant than the previously known curve of rank 14 appearing in [5]. The x-coordinates of a set of generators for each of these curves is given in Appendix B.3.

11. Curves with torsion subgroup $\mathbb{Z}/4\mathbb{Z}$

We searched a pair of families each having Mordell–Weil group $\mathbb{Z}^4 \times \mathbb{Z}/4\mathbb{Z}$, both of which are elliptic fibrations of the singular K3 surface of discriminant -163. The first fibration is given by the equation

$$\begin{aligned}\mathcal{E}_1 : y^2 + (8t-1)(32t+7)xy + 8(8t-1)(32t+7)(t+1)(15t-8)(31t-7)y \\ = x^3 + 8(t+1)(15t-8)(31t-7)x^2 \quad (5)\end{aligned}$$

and appears (with a typo) in [8]. A choice of x-coordinates defining four independent sections is given by

$$(-15/4)(t+1)(31t-7)(32t+7), \quad (8t-1)(15t-8)(31t-7)(32t+7),$$
$$-(t+1)(8t-1)(15t-8)(32t+7), \quad -4(t+1)(2t+5)(15t-8)(32t+7).$$

The second fibration is given by the equation

$$\begin{aligned}\mathcal{E}_2 : y^2 - 8(80t+9)xy - 16(80t+9)(t-2)(2t-1)(18t-1)(2t-81)y \\ = x^3 + 2(t-2)(2t-1)(18t-1)(2t-81)x^2 \quad (6)\end{aligned}$$

and will appear in [10]. A choice of x-coordinates defining four independent sections is given by

$$154(t-2)(2t-1)(18t-1), \quad -1456(t-2)(2t-1)(2t-81),$$
$$16(t-2)(2t-81)(22t+21), \quad 6(2t-5)(t-2)(2t-81)(18t-1).$$

The previous rank record for torsion group $\mathbb{Z}/4\mathbb{Z}$ was 12, attained by two curves in the family $\mathcal{E}_1$, found by Elkies in 2006 ($t = 18745/6321$) and Dujella and Peral in 2014 ($t = -13083/72895$). We searched up to height 2^{22} on $\mathcal{E}_1$ and found three rank 13 specializations at $t = -1086829/638219$, $t = -2856967/190447$, and $t = 973215/3135431$, as well as 76 rank 12 specializations. Of the rank 12 specializations, the one with smallest conductor occurs at $t = -447577/2601952$ ($N_{E_t} \approx 2^{153.41}$) and the one with smallest discriminant occurs at $t = 83497/251378$ ($|\Delta_{E_t}| \approx 2^{392.96}$). Respectively, these have smaller conductor and discriminant than the previously known rank 12 curves.

We searched up to height 2^{22} on $\mathcal{E}_2$ and were unable to find any specializations of rank 13, though we did find 32 having rank 12. Among these, the specialization with smallest conductor and discriminant appears at $t = -16307/121584$ ($N_{E_t} \approx 2^{161.21}$ and $|\Delta_{E_t}| \approx 2^{433.71}$).

Minimal models and x-coordinates of a set of generators for each of the rank 13 specializations are given in Appendix B.4.

12. Curves with torsion subgroup $\mathbb{Z}/5\mathbb{Z}$

As noted in Section 4, for the group $\mathbb{Z}/5\mathbb{Z}$, we chose to search for good specializations on the universal elliptic curve having a point of order 5, which is a rational elliptic surface. One particularly nice model for this surface is given by

$$y^2 + (t+1)xy + ty = x^3 + tx^2,$$

which has the feature that the nontrivial automorphism of $X_1(5)$ as a cover of $X_0(5)$ is given by $t \mapsto -1/t$.

Changing t to $-1/t$ yields the same curve with a different choice of generator of its torsion group. This allowed us to limit our search to $t > 0$. We searched for t up to height 2^{29} on this surface, finding a single rank 9 curve at $t = 266165145/442317512$.

We also found 392 rank 8 specializations, three of which were previously known. Of these, the curve we found with smallest conductor appears at $t = 1809535/5292661$ ($N_{E_t} \approx 2^{85.86}$) and the curve we found with smallest discriminant appears at $t = 5167107/723695$ ($|\Delta_{E_t}| \approx 2^{254.77}$). Each of these has both smaller conductor and discriminant than all of the previously known rank 8 curves.

Minimal models and x-coordinates of a set of generators for the rank 9 specialization and the smallest conductor and discriminant rank 8 specializations appear in Appendix B.5.

13. Curves with torsion subgroup $\mathbb{Z}/6\mathbb{Z}$

As was the case for $\mathbb{Z}/5\mathbb{Z}$, we chose to search for good specializations on the universal elliptic curve having a point of order 6, which is a rational elliptic surface. A model for this surface is given by

$$y^2 + txy + (t+2)y = x^3,$$

with torsion points of order 2, 3, 6 at $(x, y) = (-1, -1)$, $(0, 0)$, $(t+2, t+2)$, respectively.

We searched for good specializations of this model in the region $t = a/b$ with $0 < a < 2^{25}$ and $-2^{26} < b < 2^{26}$. In this case, the skewed search region was a fortuitous accident, rather than a deliberate choice. We found a single rank 9 curve at $t = -22029701/37178488$ as well as 71 rank 8 specializations, all but one of which appear to be previously unknown. The rank 8 curve with the smallest conductor and smallest discriminant appears at $t = 6308333/1000939$ ($N_{E_t} \approx 2^{81.96}$ and $|\Delta_{E_t}| \approx 2^{253.07}$). Its 2-isogenous curve that appears at $t = -24627934/8310211$ shares the same conductor, but has larger discriminant.

Minimal models and x-coordinates of a set of generators for the rank 9 specialization and the smallest conductor/discriminant rank 8 specialization appear in Appendix B.6.

Remark. In retrospect, we could have taken advantage of the involution $w_2 : t \mapsto -(2t+12)/(t+2)$, for which $E_{w_2(t)}$ is the curve E'_t which is 2-isogenous with E_t, and thus also has torsion subgroup $\mathbb{Z}/6\mathbb{Z}$. This would let us restrict our search area to $-4 < t < 2$. In partial compensation, we could compare the scores of t and $w_2(t)$ to corroborate that we are computing these scores correctly.

14. Curves with torsion subgroup $\mathbb{Z}/7\mathbb{Z}$

As noted in Section 4, for the group $\mathbb{Z}/7\mathbb{Z}$, we chose to search for good specializations of the universal elliptic curve having a point of order 7. Unlike the groups $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$, the universal elliptic curve having a point of order 7 is a K3 surface rather than a rational one.

A model for this curve is given by

$$y^2 + (-t^2+t+1)xy + (-t^3+t^2)y = x^3 + (-t^3+t^2)x^2$$

(see, e.g., [28, p. 195]).

The modular curve $X_1(7)$ has two nontrivial automorphisms as a cover of $X_0(7)$. These correspond to the transformations $t \mapsto 1 - 1/t$ and $t \mapsto -1/(t-1)$ on this surface which allowed us to restrict ourselves to considering $0 < t < 1$.

We searched up to height 2^{20} on this model and found a single specialization of rank 6 at $t = -748328/820369$. A minimal model and the set of x-coordinates of a set of generators of this specialization are given in Appendix B.7.

Remark. In addition to the group $\mathbb{Z}/7\mathbb{Z}$, there are two other groups G, namely, $G = \mathbb{Z}/8\mathbb{Z}$ and $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, for which the universal elliptic curve E with a copy of G in $E(\mathbb{Q})$ is a K3 surface. The rank record for each of these two G is 6, and [5] lists several curves attaining this record in each case. We looked for curves of larger rank for each of these torsion subgroups by searching on a model of the corresponding universal elliptic curve, but failed to find any specialization having rank greater than 6. We suspect that the reason we found a record-breaking curve for $\mathbb{Z}/7\mathbb{Z}$ but not for $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is simply that the previous record was lower for $\mathbb{Z}/7\mathbb{Z}$.

Appendix A: Points on $\mathcal{E}_u/\mathbb{Q}(t)$

Recall that in (3) and (4) we exhibit A and $B_1, \dots, B_8$ in $\mathbb{Q}[t, u]$ such that $\mathcal{E}_u/\mathbb{Q}(t)$ has Weierstrass equation $y^2 = x^3 + 2Ax^2 + Bx$ where $B = \prod_{i=1}^{8} B_i$. The minimal height of a nontorsion section is 2, attained by 70 pairs $(x, \pm y)$ with $x, y \in \mathbb{Q}(u, \sqrt{5-u^2})[t]$. We find that 58 of the 70 pairs have $x, y \in \mathbb{Q}(u)[t]$; these generate a Mordell–Weil subgroup of rank 8. One simple choice of generators of this subgroup consists of points with x-coordinates

$$\begin{aligned} &-B_1B_2B_3B_6, \quad -B_1B_2B_4B_5, \quad 4B_1B_2B_5B_6, \quad B_1B_3B_4B_6, \\ &-B_1B_3B_4B_7, \quad B_1B_3B_4B_8, \quad B_1B_3B_5B_6, \quad -B_1B_5B_6B_7. \end{aligned} \tag{7}$$

Extending $\mathbb{Q}(u)$ by $\sqrt{5-u^2}$ yields $\mathbb{Q}(m)$ where m is a rational coordinate on the parametrizing Shimura curve, with

$$u = 2\frac{m^2 - m - 1}{m^2 + 1}, \qquad (5 - u^2)^{1/2} = \pm\frac{m^2 + 4m - 1}{m^2 + 1}; \tag{8}$$

then adding $-(m-1)^2 B_1B_2B_3B_8$ to the list (7) gives x-coordinates of 9 Mordell–Weil generators modulo torsion. The Gram matrix of canonical height pairings is

$$\frac{1}{2}\begin{bmatrix} 4 & 0 & 1 & -1 & 0 & 2 & -1 & 0 & 1 \\ 0 & 4 & -1 & -2 & 0 & 2 & -2 & 0 & 0 \\ 1 & -1 & 4 & 0 & -1 & 1 & -1 & 1 & 2 \\ -1 & -2 & 0 & 4 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 4 & 1 & 0 & -2 & 0 \\ 2 & 2 & 1 & -1 & 1 & 4 & -2 & -1 & 1 \\ -1 & -2 & -1 & 1 & 0 & -2 & 4 & 1 & 0 \\ 0 & 0 & 1 & 0 & -2 & -1 & 1 & 4 & 1 \\ 1 & 0 & 2 & 0 & 0 & 1 & 0 & 1 & 4 \end{bmatrix}, \tag{9}$$

with determinant 115/16.

Appendix B: Models for record breaking curves

B.1. ***Overview.*** This section gives minimal integral models for each of the record breaking curves we discovered, along with the x-coordinates of a set of points that, at a minimum, generates the torsion-free part of each of them. We expect that this set of points generates the full torsion-free part of each curve given, but have not tried to prove this rigorously.

By common convention we use a vector $(a_1, a_2, a_3, a_4, a_6)$ to mean the extended Weierstrass model

$$y^2 + a_1xy + a_3x = x^3 + a_2x + a_4x + a_6$$

whose coefficients are the vector's entries. We usually depart from another common convention that chooses the model with $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{-1, 0, 1\}$. Such models have the advantage of being unique, but for curves with nontrivial torsion there may be one or more other choices that put a torsion point at $(x, y) = (0, 0)$ and have a coefficient vector with noticeably fewer digits (for starters $a_6 = 0$ if $(0, 0)$ is on the curve).

When possible we give a generating set of $E(\mathbb{Q})$ mod $E(\mathbb{Q})_{\text{tors}}$ consisting of integral points of small height. For most of our curves there are plenty of such points to choose from, even though there can be other curves with the same torsion group and somewhat lower rank that have even more integral points.

B.2. $\mathbb{Z}/2\mathbb{Z}$**.** A minimal model for the rank 20 curve having $\mathbb{Z}/2\mathbb{Z}$ torsion has coefficients

$$\begin{aligned}&(1, -1, 1, -244537673336319601463803487168961769270757573821859853707,\\ &\qquad 961710182053183034546222979258806817743270682028964434238957830989898438151121499931).\end{aligned}$$

Here we reluctantly give a model with small a_1, a_2, a_3 and huge a_4, a_6, because the torsion point has $x = -6928858868611170267862561672 5/4$ and thus cannot be put at the origin on a minimal model.[2]

One choice of 20 points that generate its Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rr}
-5976635286513806621064126789, & 5954163887874902594437665 91,\\
24345628722931082751070290 75, & 35130740273444351711409789 81,\\
39968214524905175813332741 9, & -10714754038296881855524018251,\\
-16034220456847626275437501599, & 11858286723552143924257991 31,\\
-11190697582885409770718510409, & 26343164463106803320421222 61,\\
642221499783690555694347255 91, & 23945425437351916471937562579,\\
130941144005832954327563466 51, & 268977633454108991742455223651 1,\\
-262701403897994182933186146 9, & 113605800622499112413124359631,\\
-73649387488418077577736257 09, & -142982229271592849141800723 49,\\
785686589410787916270883192839, & -22501704910798392589349007 09.
\end{array}$$

Here and later we list generators in increasing order by canonical height.

[2] The coefficients $(2, -207865766058335108035876850179, 0, 1049012279295838632209367044442722387731922776108179521 7921, 0)$ give a model with smaller coefficients that puts the torsion point at $(0, 0)$ but is not minimal at 2.

A minimal model for the rank 19 curve with $\mathbb{Z}/2\mathbb{Z}$ torsion having smallest known discriminant has coefficients

$$(1, 4040549489437705068551042, 0, 3909667311181520606577323723458725658233129 6000, 0).$$

One choice of 19 points that generate its Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rr}
-361329442609813519987860 0, & 284077053735716552925900, \\
-697863438918158206668 00, & 64090788994348705875 00, \\
4711243262341394854929360, & -2008620344802957879903 00, \\
4974670401368392643160 0, & 1283007628272047952000, \\
6012436806643061846134 20, & 16816790703861093580060 14, \\
-1786743474392042001621 50, & -1400584660676007289711 80, \\
449059225193074157376 0, & -124541800924686435200625 0, \\
2394359380472424100507 20, & -261592604251110288280800 0, \\
-366282047410641864153600 0, & 308679854892675472378120, \\
-121301193731400473856 00. &
\end{array}$$

B.3. $\mathbb{Z}/3\mathbb{Z}$**.** The rank 15 elliptic curve with coefficient vector

$$(490738465519, 0, -4328027291801888780356705224235578 75, 0, 0)$$

has a 3-torsion point at $(x, y) = (0, 0)$. One choice of 15 points that generate its Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rrr}
4140822948731860002991 47, & -4610760379586196913759 50, & 136016697778663191410466, \\
5798110741945694475507 75, & 4156065765459153070875350, & -3792564368564900832226 05, \\
-48025726620075720109912 5, & 6268793496869947592713 50, & 3194021981679225796758 75, \\
9987762741068630814895872, & 10255590769784537981873 16, & 1771004712378818165404837 5, \\
23642683057088944606594 2, & -1628606814467216221105 65, & 1093411474853808475876875.
\end{array}$$

The rank 14 elliptic curve with coefficient vector

$$(6244332976, 0, -220442125064192217455663037 5, 0, 0)$$

has a 3-torsion point at $(x, y) = (0, 0)$. One choice of 14 points that generate its Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rrrr}
2907919170263662, & -65199074165293250, & 71604990115331040, & 77567806466944000, \\
108999498650081840, & 169617569990697350, & -171009947870163008, & -204167066230390100, \\
-240427032442334750, & 243676691791782250, & -256142889038646510, & -276580713950955750, \\
368313341140417750, & -449841531945448000. & &
\end{array}$$

B.4. $\mathbb{Z}/4\mathbb{Z}$**.** The first rank 13 curve with $\mathbb{Z}/4\mathbb{Z}$ torsion has a minimal model with coefficient vector

$$\begin{array}{l}
(282887999996745, -1871148179781457712818452480, \\
\qquad\qquad -52932536627592642213859774030701593717760 0, 0, 0)
\end{array}$$

and a 4-torsion point at $(x, y) = (0, 0)$. One choice of 13 points that generate its Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rr}
37563104221873287230436120000, & 1241851783771179145432296000, \\
1992140999686088390294877150, & 3092104273799154268335926380, \\
-21195532433936174709304166400, & -1464098167733086800531916800, \\
1670745991840921221771294750, & 1252355926117744178967180450, \\
-1960920553671074388872220170, & 13752931853472754996630572800, \\
2549902537861429590505036800, & 32729192217380282521063038727 14, \\
102225511700163143939329914880. &
\end{array}$$

The second rank 13 curve with $\mathbb{Z}/4\mathbb{Z}$ torsion has a minimal model with coefficient vector

$$\begin{aligned}(230691818102905, -200100346570723590045845120,& \\ -4616151275342161672702302511289585 2073600, 0, 0)&\end{aligned}$$

and a 4-torsion point at $(x, y) = (0, 0)$. One choice of 13 points that generate its Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rr}
1904128696297486292067885 00, & -11655521125151390350616252280, \\
-10482658909728296079200226100, & -2052538702327974211090080 00, \\
1932305568286471635228576 00, & 2390337099874364874239977850, \\
-10561431236301791011714683300, & -1195165694989063921020955200, \\
876665740401972718169616600, & -99112055810721390011710344, \\
-6556600091394826719688358 4, & 166949951644450209072942720, \\
-26328612670314620364001050. &
\end{array}$$

The third rank 13 curve with $\mathbb{Z}/4\mathbb{Z}$ torsion has a minimal model with coefficient vector

$$\begin{aligned}(246888014319233, -888428556659021986550032563 2,& \\ -2193423622180481268696018169961040300480256, 0, 0)&\end{aligned}$$

and a 4-torsion point at $(x, y) = (0, 0)$. One choice of 13 points that generate its Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rr}
-9685160842346410587093702 32, & -1333726837303108113451614080, \\
1792794868671671366043266816, & 2362595876319902581142656768, \\
-2746004168634841009972934984, & 3469325866293712913010729024, \\
3644805279133239447459855232, & 4449372053406414078540323280, \\
-4537829698895530474950049368, & 5156996081584183666047796032, \\
5789474008645490085082165824, & 5912795841516183863849831680, \\
10555676267250916670215460568. &
\end{array}$$

B.5. $\mathbb{Z}/5\mathbb{Z}$. The rank 9 curve with $\mathbb{Z}/5\mathbb{Z}$ torsion has a minimal model with coefficient vector

$$(708482657, 117729504717519240, 52073821615645373048930880, 0, 0).$$

The torsion group is generated by $(x, y) = (0, 0)$. One choice of 9 points that generate the Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rrr} -95393153480017302, & 172086875265878580, & -12976225316716116, \\ 53638875373006560, & -147039491421732240, & 46489325594722920, \\ -148084847397297720, & 215103037614492081 60, & 79310646743033160. \end{array}$$

The rank 8 curve with $\mathbb{Z}/5\mathbb{Z}$ torsion having smallest known conductor has a minimal model with coefficient vector

$$(7102196, 9577255322635, 5068916573315268173 5, 0, 0).$$

The torsion group is generated by $(x, y) = (0, 0)$. One choice of 8 points that generate the Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rrrr} -11217531799903, & -10836503720185, & -4357099419673, & 1401549559410, \\ 256939125827615, & -10247328030940, & -6060818514894, & -6697297034428. \end{array}$$

The rank 8 curve with $\mathbb{Z}/5\mathbb{Z}$ torsion having smallest known discriminant has a minimal model with coefficient vector

$$(5890802, 3739409500365, 270619195836664867 5, 0, 0).$$

The torsion group is generated by $(x, y) = (0, 0)$. One choice of 8 points that generate the Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rrrr} -21207376737, & 37660080920, & -89104376475, & 100531079550, \\ 117291419735, & -120660570135, & 148808336985, & -214614453600. \end{array}$$

B.6. $\mathbb{Z}/6\mathbb{Z}$. The rank 9 curve with $\mathbb{Z}/6\mathbb{Z}$ torsion has a minimal model with coefficient vector

$$(-22029701, 0, 72328851024410157777600, 0, 0).$$

The torsion group is generated by $(x, y) = (1945448965660200, 72328851024410157777600)$; multiplying this point by 2 yields the 3-torsion point $(0, 0)$. One choice of 9 points that generate the Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rrr} 749629491053742, & 6092756193428190, & -1380249411088240, \\ -1067429532233440, & 17453290957977303 0, & 949536320242950, \\ 1079473135677300, & 24157188371048640, & 3112751229126000. \end{array}$$

The rank 8 curve with $\mathbb{Z}/6\mathbb{Z}$ torsion and smallest known conductor and discriminant has a minimal model with coefficient vector

$$(6308333, 0, 8325824903545553131, 0, 0).$$

The torsion group is generated by $(x, y) = (8318014288129, 8325824903545553131)$; multiplying this point by 2 yields the 3-torsion point $(0, 0)$. One choice of 8 points that generate the Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{rrrr} -204062889121, & 211687889245, & -403788801990, & -410295468023, \\ -733395115518, & -823562706096, & -859172099915, & -2828410292799. \end{array}$$

B.7. $\mathbb{Z}/7\mathbb{Z}$. The rank 6 curve with $\mathbb{Z}/7\mathbb{Z}$ torsion has a minimal model with coefficient vector

$$(-500894592455, 7206631203310599177237 12, 485010096730715360294683087532269632, 0, 0).$$

The torsion group is generated by $(x, y) = (0, 0)$. One choice of 6 points that generate the Mordell–Weil group modulo torsion has x-coordinates

$$\begin{array}{ll} -8632402194557597083438 72, & 147841500613888155442368, \\ -655405721270483784258504, & 227328163133810400709740, \\ 177585911391567339712811 76, & 445789440416234739212776555850 5920/79519^2. \end{array}$$

The large final generator is inevitable: the first five generators have canonical heights between 15.434 and 19.431, but the last generator must have height at least 42.058 (we have made the minimal choice, and with the smallest possible denominator among its seven torsion translates).

Acknowledgements

We thank Tom Fisher for pointing out that we could easily compute p-descents via isogeny on the curves having torsion subgroups $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z}$. We thank the referees for making numerous helpful comments and suggestions. We also thank Andrej Dujella for alerting us to an inaccuracy in our original manuscript.

References

[1] Monique van Beek. *Computing the Cassels-Tate pairing*. Doctoral dissertation. University of Cambridge, 2015.

[2] Monique van Beek and Tom Fisher. *Computing the Cassels–Tate pairing on 3-isogeny Selmer groups via cubic norm equations*. Acta Arithmetica Vol. 185 (2018): 367–396.

[3] Bryan Birch and H. Peter F. Swinnerton-Dyer. *Notes on elliptic curves. I.* J. Reine Angew. Math Vol. 212.7 (1963): 7–25.

[4] Wieb Bosma, John Cannon, and Catherine Playoust. *The Magma algebra system. I. The user language*. J. Symbolic Comput. Vol 24 (1997): 235–265.

[5] Andrej Dujella. *High rank elliptic curves with prescribed torsion.* 2020, https://web.math.pmf.unizg.hr/~duje/tors/tors.html.

[6] Andrej Dujella, Juan Carlos Peral, and Petra Tadić. *Elliptic curves with torsion group $\mathbb{Z}/6\mathbb{Z}$*. Glasnik matematički Vol. 51.2 (2016): 321–333.

[7] Noam D. Elkies. *Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction*. International Algorithmic Number Theory Symposium. Springer LNCS Vol. 1838. Springer, Berlin, Heidelberg (2000): 33–63.

[8] Noam D. Elkies. *Three lectures on elliptic surfaces and curves of high rank*. arXiv:0709.2908

[9] Noam D. Elkies. *Shimura curve computations via K3 surfaces of Néron–Severi rank at least 19*, Algorithmic Number Theory - ANTS VIII. Springer LNCS Vol. 5001. Springer, Berlin, Heidelberg (2008): 137–147.

[10] Noam D. Elkies. The 167889 even lattices of rank 18 and discriminant 163, and the 167889 elliptic fibrations of the singular K3 surface of discriminant −163. Preprint, 2020.

[11] Noam D. Elkies and Abhinav Kumar. *K3 surfaces and equations for Hilbert modular surfaces*, Algebra and Number Theory Vol. 8.10 (2014): 2297–2411.

[12] Stéfane Fermigier. *Une courbe elliptique définie sur $\mathbb{Q}$ de rang $\geq$ 22*. Acta Arithmetica Vol. 82.4 (1997): 359–363.

[13] Tom Fisher. *Higher descents on an elliptic curve with a rational 2-torsion point*. Mathematics of Computation Vol. 86.307 (2017): 2493–2518.

[14] Shoichi Kihara. *On the rank of the elliptic curves with a rational point of order 6*. Proceedings of the Japan Academy, Series A, Mathematical Sciences Vol. 82.7 (2006): 81–82.

[15] Odile Lecacheux. *Rang de courbes elliptiques sur $\mathbb{Q}$ avec un groupe de torsion isomorphe à $\mathbb{Z}/5\mathbb{Z}$*. Comptes Rendus de l'Académie des Sciences. Série 1, Mathématique Vol. 332.1 (2001): 1–6.

[16] Barry Mazur. *Modular curves and the Eisenstein ideal*. Publications Mathématiques de l'Institut des Hautes Études Scientifiques Vol 47.1 (1977): 33–186.

[17] Jean-François Mestre. *Construction d'une courbe elliptique de rang* ≥ 12. Comptes rendus de l'Académie des sciences. Série 1, Mathématique Vol. 295.12 (1982): 643–644.

[18] Jean-François Mestre. *Courbes elliptiques et formules explicites*. Séminaire de théorie des nombres de Grenoble Vol. 10 (1982): 1–10.

[19] Jean-François Mestre. *Courbes elliptiques de rang* ≥ 12 *sur* $\mathbb{Q}(T)$. Comptes rendus de l'Académie des sciences. Série 1, Mathématique Vol. 313.4 (1991): 171–174.

[20] Jean-François Mestre. *Un exemple de courbe elliptique sur $\mathbb{Q}$ de rang* ≥ 15. Comptes rendus de l'Académie des sciences. Série 1, Mathématique Vol. 314.6 (1992): 453–455.

[21] Louis Mordell. *On the rational solutions of the indeterminate equation of the third and fourth degree*. Proceedings of the Cambridge Philosophical Society. Vol. 21 (1922): 179–192.

[22] Brian Murphy. *Modelling the yield of number field sieve polynomials*. Algorithmic Number Theory - ANTS III, Springer LNCS Vol. 1443. Springer, Berlin, Heidelberg, (1998): 137–150.

[23] Koh-Ichi Nagao. *Examples of elliptic curves over $\mathbb{Q}$ with rank* ≥ 17. Proceedings of the Japan Academy, Series A, Mathematical Sciences Vol. 68.9 (1992): 287–289.

[24] Koh-ichi Nagao. *An example of elliptic curve over $\mathbb{Q}$ with rank* ≥ 20. Proceedings of the Japan Academy, Series A, Mathematical Sciences Vol. 69.8 (1993): 291–293.

[25] Jennifer Park, Bjorn Poonen, Melanie Matchett Wood, and John Voight. *A heuristic for boundedness of ranks of elliptic curves.* To appear in Journal of the European Mathematical Society.

[26] Henri Poincaré. *Sur les propriétés arithmétiques des courbes algébriques*. J. Pures Appl. Math. Vol. 7.5 (1901): 161–234.

[27] Joseph H. Silverman. *Heights and the specialization map for families of abelian varieties*. Journal für Mathematik. Band 342 (1983): 197–211.

[28] John Tate. *The arithmetic of elliptic curves*. Inventiones Mathematicæ Vol. 23 (1974): 179–206.

[29] Maksym Voznyy. Personal communication. August 2020.

[30] Mark Watkins et al. *Ranks of quadratic twists of elliptic curves*. Publications Mathématiques de Besançon Vol. 2 (2014): 63–98.

[31] Mark Watkins. *A discursus on 21 as a bound for ranks of elliptic curves over $\mathbb{Q}$, and sundry related topics*. August 20, 2015. Available at http://magma.maths.usyd.edu.au/~watkins/papers/DISCURSUS.pdf.

Received 24 Feb 2020.

NOAM D. ELKIES: elkies@math.harvard.edu
Department of Mathematics, Harvard University, Cambridge, MA, United States

ZEV KLAGSBRUN: zdklags@ccrwest.org
Center for Communications Research, San Diego, CA, United States

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article "Supersingular curves with small noninteger endomorphisms", by Jonathan Love and Dan Boneh (see p. 9).

Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.

msp

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS