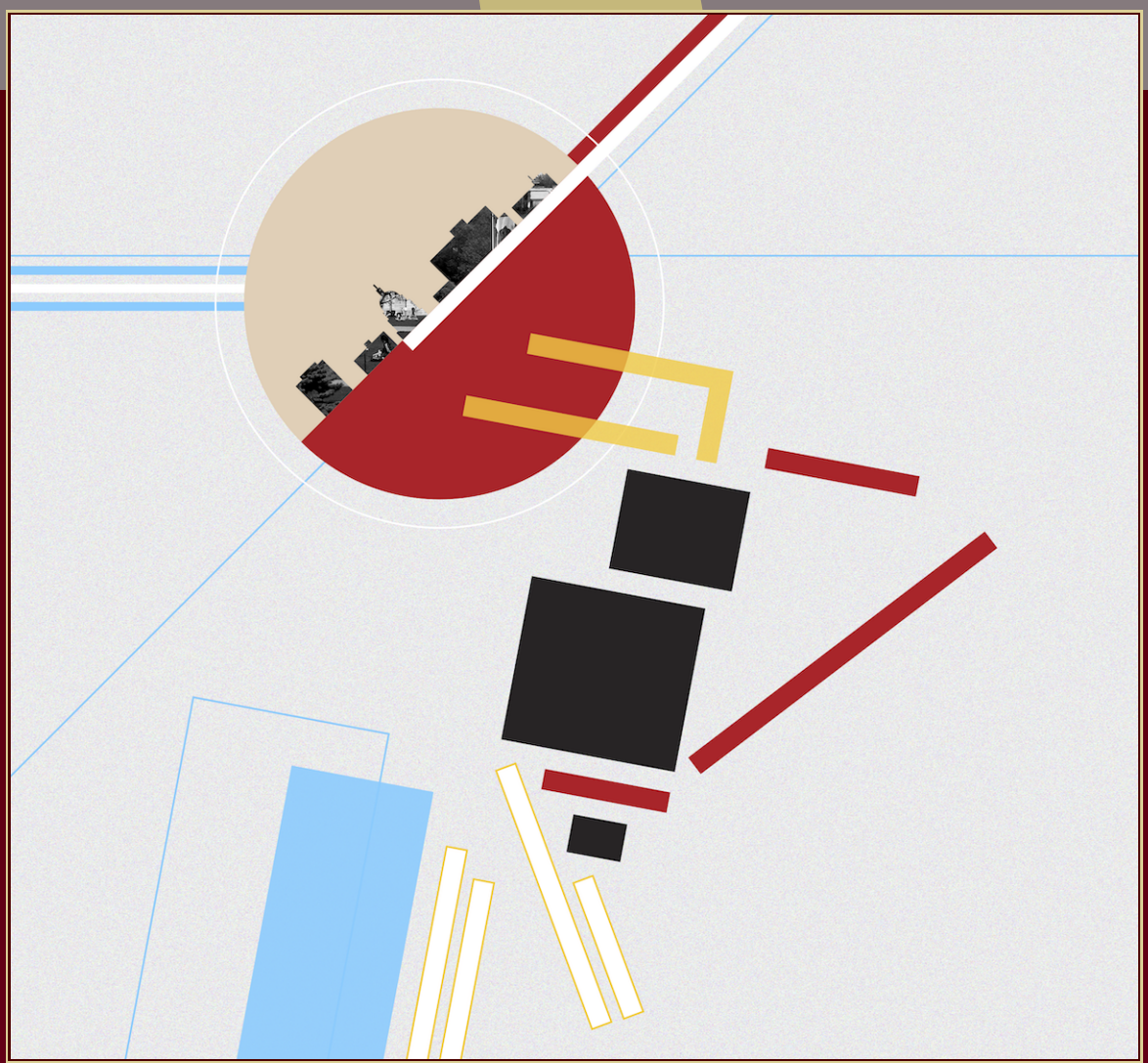
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

Ranks, 2-Selmer groups, and Tamagawa numbers of elliptic curves with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$-torsion

Stephanie Chan, Jeroen Hanselman, and Wanlin Li



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.173

msp

Ranks, 2-Selmer groups, and Tamagawa numbers of elliptic curves with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$-torsion

Stephanie Chan, Jeroen Hanselman, and Wanlin Li

In 2016, Balakrishnan, Ho, Kaplan, Spicer, Stein and Weigandt produced a database of elliptic curves over $\mathbb{Q}$ ordered by height in which they computed the rank, the size of the 2-Selmer group, and other arithmetic invariants. They observed that after a certain point, the average rank seemed to decrease as the height increased. Here we consider the family of elliptic curves over $\mathbb{Q}$ whose rational torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Conditional on GRH and BSD, we compute the rank of 92% of the 202,461 curves with parameter height less than 10^3. We also compute the size of the 2-Selmer group and the Tamagawa product, and prove that their averages tend to infinity for this family.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$. After a suitable choice of isomorphism, we can always express such a curve in its short Weierstrass form:

$$E : y^2 = x^3 + a_4 x + a_6,$$

with $a_4, a_6 \in \mathbb{Z}$. Using this description, we define the naive height of the curve E as

$$h(E) := \max\{4|a_4|^3, 27a_6^2\}.$$

In [1], the authors created an exhaustive database of isomorphism classes of elliptic curves with naive height up to $2.7 \cdot 10^{10}$, which contained a total of 238,764,310 curves. For each elliptic curve in this database, they computed the minimal model, the torsion subgroup, the conductor, the Tamagawa product, the rank, and the size of the 2-Selmer group. They plotted the average rank of the curves up to a certain height. Initially the average rank seemed to be an increasing function, but around a naive height of 10^9, they observed a turnaround point, where the average rank seemed to start decreasing as the height was increasing.

In this database however, there were no elliptic curves recorded with rational torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, which is the largest possible torsion subgroup for elliptic curves over $\mathbb{Q}$. The curve with minimal naive height that has such a torsion group has Weierstrass form $y^2 = x^3 - 1386747x + 368636886$ and its naive height is $10667230914617018892 \approx 1.07 \cdot 10^{19}$.

MSC2010: 11G05, 11Y40.
Keywords: elliptic curve, rank, Selmer group, Tamagawa number.

In this paper, we describe a similar database for the family of elliptic curves over $\mathbb{Q}$ whose rational torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. We can parametrize this family in the following way:

$$\mathcal{F} := \left\{ E : y^2 = x(x+1)(x+u^4) \;\middle|\; u = \frac{2t}{t^2-1},\ t \in \mathbb{Q} \setminus \{0, 1\} \right\}.$$

We call t the parameter of the curve and write $t = a/b$ for coprime integers a, b. This particular parametrization was provided by Bartosz Naskręcki, resulting from ideas in [16]. The family inherits a height function from its parametrization. For any $E \in \mathcal{F}$, we define the parameter height $H(E) := \max\{|a|, |b|\}$. For each isomorphism class of curves in this family, we will only consider the model in $\mathcal{F}$ for which H is minimal. From now on, we will call the family of curves represented by elements of $\mathcal{F}$ the $(2, 8)$-torsion family.

We use the parameter height, as it makes it easier to enumerate and compare curves in our family. The naive height of the curves in our family is very large, as could already be seen in the example mentioned above. We prove in Section 2 that

$$0.559 \cdot h(E)^{1/48} < H(E) < 0.672 \cdot h(E)^{1/48}.$$

We also show that the parameter height controls the size of the conductor $N(E)$:

$$N(E) < 1.161 \cdot H(E)^{10}.$$

From now on, we will use the term *height* to refer to the parameter height.

There are several reasons to consider the $(2, 8)$-torsion family. First, based on the relation between the parameter height and the naive height, restricting to this family allows us to quickly see curves of large naive height. Another advantage is that the existence of the rational torsion structure makes it easier to carry out 2-descent.

To provide an example, the 2000th curve in our database has parameter $t = \frac{98}{99}$, naive height $6.39 \cdot 10^{107}$ and conductor $6.65 \cdot 10^{17}$. It would be more difficult to determine the rank for a curve of similar size without any special structure, and currently it would not be feasible to carry out such calculations in bulk.

In our family, we enumerated all 202,461 isomorphism classes of curves with height less than 1000. The average rank function seems to achieve its maximum at height 24, at the 121st curve, where the average rank peaks at 0.744. Among these, we determined the rank for 186,876 classes, conditional on GRH and BSD.

This particular family of elliptic curves was also studied in [7] and [12]. In [7], the authors were in search of rank 4 curves, but were unable to find any. To date, no rank 4 curve has yet been found in this family. In [12], the authors obtained statistical results on the 2-Selmer group, similar to our data in Section 5B.

Main results. We found that curves with height up to 100 in the $(2, 8)$-torsion family have average rank 0.626 (Figure 2 in Section 5A) and with height up to 1000 have average rank between 0.508 and 0.663

(Figure 3 in Section 5A). The first curves in the $(2,8)$-torsion family with given rank r are

$$r=0\colon y^2=x^3-1386747x+368636886 \qquad \left(t=\tfrac{1}{2}\right),$$
$$r=1\colon y^2=x^3-64052311707x+6090910426477494 \qquad \left(t=\tfrac{1}{4}\right),$$
$$r=2\colon y^2=x^3-4288450677931298 7x+337937756079527 4084396534 \qquad \left(t=\tfrac{5}{8}\right),$$
$$r=3\colon y^2=x^3-2040672855995450048 4507x+1121060630379489735235148874483894 \qquad \left(t=\tfrac{12}{17}\right).$$

We found that no rank-4 curves can exist with height below 1000.

The curve with rank 3 with the greatest height found in our database has parameter $t=\frac{841}{1018}$; its global minimal model is

$$y^2+xy=x^3-153729452329750732156924947255990241355929710255 0x +7336366246333132846308148525227910550151380147382941246791656800601001 32.$$

This curve was found when we tried to compute the 2-Selmer rank of curves beyond height 1000. Currently, the curve with maximal height on the list of elliptic curves with high rank maintained by Dujella [10] has parameter $\frac{352}{1017}$.

The average size of the 2-Selmer group seems to be increasing rather slowly, but steadily. We prove the following theorem, which is an analogue of a result by Lemke Oliver and Klagsbrun for the family of elliptic curves with 2-torsion [15].

Theorem 6.3. *The average size of the* 2*-Selmer group tends to infinity in the* $(2,8)$*-torsion family.*

Similarly, observing the data on the average Tamagawa product suggested the following theorem that we prove in Section 6A:

Theorem 6.1. *The average Tamagawa product in the* $(2,8)$*-torsion family up to height* N *has order of magnitude* $(\log N)^{33}$.

Outline of the paper. In Section 2, we provide some properties of the $(2,8)$-torsion family related to our parametrization. In Section 3, we recall general results and conjectures related to ranks of elliptic curves. In Section 4, we discuss the computational methods we use. Section 5 contains the data we obtained and our analysis of the data. In Section 6, we prove that the average Tamagawa product and the average size of the 2-Selmer group tends to infinity for this family.

2. Some preliminary properties of the (2 , 8)-torsion family

In this section, we discuss the parametrization for the $(2,8)$-torsion family. We also show how the parameter height is related to the naive height and the conductor.

2A. ***The parametrization.*** By expressing the torsion points explicitly, one can check that any curve with $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$-torsion can be described as an element of $\mathcal{F}$. Conversely, given a curve in $\mathcal{F}$, it is a

straightforward calculation to verify that

$$\left(\frac{2u}{(t+1)^2}, \frac{4t(t^2+2t-1)(t^2+1)}{(t+1)^5(t-1)^3}\right)$$

is a point of order 8. Hence the torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

In each isomorphism class in $\mathcal{F}$, there are exactly eight different choices of t. We get these representatives using the transformations $t \mapsto -t$, $t \mapsto 1/t$ and $t \mapsto (1-t)/(1+t)$. We choose the t corresponding to a curve with minimal height. The maps $t \mapsto -t$ and $t \mapsto 1/t$ allow us to restrict $t = a/b$ to the range $(0, 1)$. Assuming $a < b$, if $a \equiv b \equiv 1 \bmod 2$, the map $t \mapsto (1-t)/(1+t)$ allows us to take parameter $t' = a'/b'$, where $a' = (b-a)/2$ and $b' = (a+b)/2$. Then t' would have a smaller height, since $a' < b' < b$. Thus, choosing $t = a/b \in (0, 1)$ with a and b coprime with different parity, we get a unique representative for each isomorphism class.

With this choice of parameter, we see that the number of curves with height n is $\phi(n)$ if n is even and $\phi(n)/2$ if n is odd, where $\phi(n)$ is the Euler totient function. By [19], we have for any $\epsilon > 0$, the estimate

$$\sum_{n \le N} \phi(n) = \frac{3}{\pi^2} N^2 + O(N(\log N)^{2/3}(\log\log N)^{4/3}).$$

Using the fact that $\phi(2n)$ is $\phi(n)$ if n is odd and $2\phi(n)$ if n is even, one can show that the total number of curves up to height N is

$$\frac{2}{\pi^2} N^2 + O(N(\log N)^{2/3}(\log\log N)^{4/3}).$$

2B. ***Naive height and parameter height.*** Let E be a curve given by the equation $y^2 = x(x+1)(x+u^4)$ in $\mathcal{F}$, where $u = 2t/(t^2-1)$ and $t = a/b$ are chosen as above. We show how the naive height and parameter height are related.

Proposition 2.1. *Let $E/\mathbb{Q}$ be an elliptic curve in $\mathcal{F}$, with naive height h and parameter height H. We have*

$$0.559 \cdot h^{1/48} < H < 0.672 \cdot h^{1/48}.$$

Proof. We start by giving a minimal Weierstrass model for our curve. Write $S = 2ab$ and $T = b^2 - a^2$, so $u = -S/T$. It follows that S and T are coprime where S is even and T is odd. We write E in short Weierstrass form $y^2 = x^3 - Ax + B$ by putting

$$A = 27(S^8 - S^4T^4 + T^8) \quad \text{and} \quad B = 27(S^4 - 2T^4)(2S^4 - T^4)(S^4 + T^4).$$

One can check that there exists no prime p such that $p^4 \mid A$ and $p^6 \mid B$; therefore this Weierstrass form is minimal. With this, the naive height of E is given by

$$h = 3^9 T^{24} \max\{4|1 - u^4 + u^8|^3, (1-2u^4)^2(2-u^4)^2(1+u^4)^2\}.$$

Since this expression is symmetric in S and T, first assume $S < T$, so that $u \in (0, 1)$. Bounding the polynomials in u, we get $3^{12} \cdot T^{24}/16 \le h \le 4 \cdot 3^9 \cdot T^{24}$. Note also, $\max(S, T) = \max(2ab, b^2 - a^2) \in$

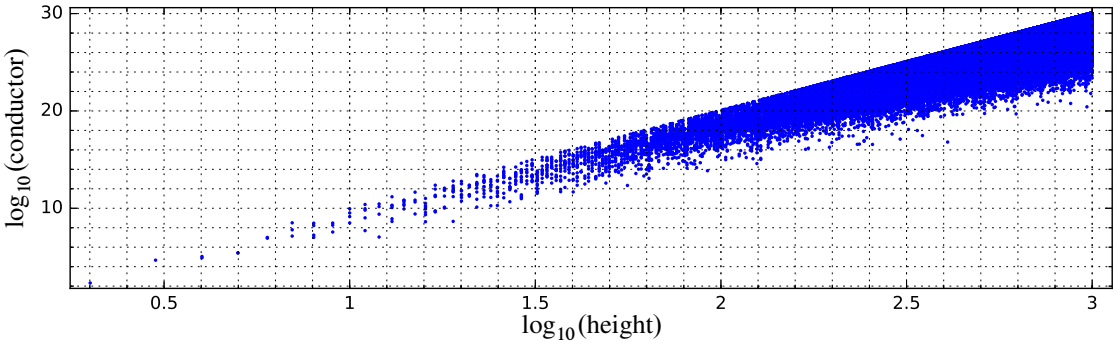


Figure 1. Conductor of isomorphism classes in the $(2, 8)$-torsion family.

$[2(\sqrt{2}-1)H^2, 2H(H-1)]$. Therefore $(\sqrt{2}-1)^{24}\cdot 3^{12}\cdot 2^{20}\cdot H^{48} < h < 3^9\cdot 2^{26}\cdot H^{48}$, which gives the result. □

2C. ***Size of the conductor.*** Consider a curve in $\mathcal{F}$ with parameter $t = a/b$, where a and b are coprime and of different parity. This curve is isomorphic to

$$E : y^2 = x(x + S^4)(x + T^4),$$

where $S = 2ab$ and $T = b^2 - a^2$ are coprime. The discriminant of E is $\Delta_E = 16S^8T^8(T^4 - S^4)^2$. By Tate's algorithm [18], this curve has bad reduction precisely at the primes dividing Δ_E, and the exponent of the conductor is always 1. Therefore the conductor of E is the product of primes dividing

$$ab(b^2-a^2)(a^2+b^2)(a^2-2ab-b^2)(a^2+2ab-b^2) = b^{10}t(1-t^2)(1+t^2)(t^2-2t-1)(t^2+2t-1).$$

The absolute value of the polynomial in t is bounded from above in the interval $(0, 1)$ by approximately 1.160. Hence $N(E) < 1.161\cdot H(E)^{10}$. See Figure 1.

3. Background

Computing the rank of an elliptic curve over a number field is a difficult problem, and while there are a number of techniques that work well in practice, there is no known algorithm to carry this out in general. Here we review the main theorems and conjectures and discuss how they can be used to give conditional results.

3A. ***The BSD conjecture.*** The most famous conjecture on ranks of elliptic curves is the Birch and Swinnerton-Dyer conjecture (BSD) [4]. Let E be an elliptic curve defined over a number field with L-function $L(s, E)$. The BSD conjecture states that the rank of E equals the order of vanishing of $L(s, E)$ at $s = 1$, which is called the *analytic rank* of E. Assuming this conjecture allows us to obtain an upper bound of the rank from the L-function.

3B. ***The minimalist conjecture and current results.*** It is believed that the root number, i.e., the sign of the functional equation of $L(s, E)$, is 1 for half of all elliptic curves and -1 for the other half. The

minimalist conjecture, initially formulated by Goldfeld [13] for the quadratic twists families, states that with respect to any reasonable ordering, half of the elliptic curves have rank 0 and half have rank 1. This would mean the average rank should tend to $\frac{1}{2}$, and 0% of elliptic curves have rank at least 2. One of our main goals is to provide numerical evidence for this conjecture for the $(2, 8)$-torsion family.

The following result of Bhargava and Shankar [2] on the upper bound of the average rank of elliptic curves provides strong evidence for the minimalist conjecture.

Theorem 3.1 (Bhargava and Shankar [2]). *The average rank of all elliptic curves over $\mathbb{Q}$ ordered by naive height is at most* 0.885.

3C. ***The Selmer group and descent.*** For each integer $n \geq 2$, the n-Selmer group $\mathrm{Sel}_n(E)$ of E over $\mathbb{Q}$ fits into an exact sequence of abelian groups

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to \mathrm{Sel}_n(E) \to Ш(E)[n] \to 0, \tag{1}$$

where $Ш(E)[n]$ denotes the n-torsion subgroup of the Tate–Shafarevich group $Ш(E)$ of E over $\mathbb{Q}$. If p is a prime, then $\mathrm{Sel}_p(E)$ is an elementary abelian p-group, whose dimension as an $\mathbb{F}_p$-vector space is called the p-Selmer rank of E, which is effectively computable and provides an upper bound on the rank via (1).

Explicitly, an element in the n-Selmer group of E can be represented by a pair (C, π), where C is a genus-1 curve which is locally soluble and π is a map defined over $\mathbb{Q}$ that makes the following diagram commute:

$$\begin{array}{ccc} C & & \\ {\scriptstyle\simeq}\downarrow & \searrow^{\pi} & \\ E & \xrightarrow[[n]]{} & E \end{array}$$

In this diagram, the vertical map $C \to E$ is an isomorphism defined over $\overline{\mathbb{Q}}$. Determining (a lower bound for) the rank of E is equivalent to finding rational points on C. If no rational point of C can be found by a search by height, we apply the method of descent repeatedly. More generally, given a rational isogeny $\phi : E \to E'$, there is a Selmer group associated to it, denoted as $\mathrm{Sel}_\phi(E)$. For the dual isogeny $\hat{\phi} : E' \to E$ of ϕ, we denote the corresponding Selmer group as $\mathrm{Sel}_{\hat{\phi}}(E')$. The following is a standard result, see for example [17, Lemma 6.1].

Theorem 3.2. *Let E and E' be elliptic curves over $\mathbb{Q}$. Suppose there exists $\phi : E \to E'$ an isogeny of degree* 2. *Then the following sequence is exact*:

$$0 \to E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2]) \to \mathrm{Sel}_\phi(E/\mathbb{Q}) \to \mathrm{Sel}_2(E/\mathbb{Q}) \to \mathrm{Sel}_{\hat{\phi}}(E'/\mathbb{Q}).$$

For $E \in \mathcal{F}$, we have $|E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2])| = 1$, which implies that

$$|\mathrm{Sel}_\phi(E/\mathbb{Q})| \leq |\mathrm{Sel}_2(E/\mathbb{Q})|.$$

Fisher [11] gives an efficient way to apply descent six times on elliptic curves with full 2-torsion structure. Moreover, since the $(2, 8)$-torsion family has $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ torsion, there are two isogenous curves with full 2-torsion structure. Applying Fisher's method to all three isogenous curves allowed us to determine the rank of more curves. Below is a picture of the isogenous curves and their torsion structures:

$$\begin{array}{ll} E & E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \\ \downarrow & \downarrow \\ E' & E'_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \\ \downarrow & \downarrow \\ E'' & E''_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{array}$$

There are also a number of recent results on the size of Selmer groups:

Theorem 3.3 (Bhargava and Shankar [3]). *For $n \leq 5$, the average size of $\mathrm{Sel}_n(E)$ for all elliptic curves $E/\mathbb{Q}$ ordered by naive height is $\sigma(n)$, the sum of divisors of n.*

The theorem implies that the average size of the 2-Selmer group converges to $\sigma(2) = 3$. However, this no longer holds for the family with nontrivial 2-torsion.

Theorem 3.4 (Klagsbrun and Lemke Oliver [15]). *The average size of $\mathrm{Sel}_2(E)$ is unbounded for the family of elliptic curves over $\mathbb{Q}$ with a torsion point of order 2 ordered by a parameter height.*[1]

Our data suggests that the average size of the 2-Selmer group is also unbounded in the $(2, 8)$-torsion family. In Section 6B, we give a proof of this fact.

3D. *The Tamagawa number.* Let E be an elliptic curve over $\mathbb{Q}$. The *Tamagawa number* is the finite index $c_p(E) := \#(E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p))$, where $E_0(\mathbb{Q}_p)$ is the subgroup of points in $E(\mathbb{Q}_p)$ which have good reduction. Each $c_p(E)$ can be easily computed from the coefficients of E using Tate's algorithm [18]. The *Tamagawa product* of E is

$$\mathcal{T}(E) = \prod_{p \leq \infty} c_p(E).$$

If there exists an isogeny $\phi : E \to E'$ of degree 2, then the *Tamagawa ratio* of E is

$$\mathcal{T}(E/E') = \frac{|\,\mathrm{Sel}_\phi(E)|}{|\,\mathrm{Sel}_{\hat{\phi}}(E')|}.$$

Consider the exact sequence induced by the isogeny ϕ:

$$0 \longrightarrow \ker(\phi) \longrightarrow E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathbb{Q}, \ker(\phi)) \longrightarrow H^1(\mathbb{Q}, E) \longrightarrow \cdots.$$

Passing to a completion at a place p, we define

$$H^1_\phi(\mathbb{Q}_p, \ker\phi) := \delta_p(E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p))) \subset H^1(\mathbb{Q}_p, \ker(\phi)).$$

[1] The parameter height used here for an elliptic curve with a 2-torsion point $E_{A,B} : y^2 = x^3 + Ax^2 + Bx$ is $\max\{|A|, B^2\}$.

Then the Tamagawa ratio can be related to the Tamagawa numbers as follows.

Theorem 3.5 (Cassels [8, Lemma 3.1]). *The Tamagawa ratio decomposes into a product of local factors as follows*:

$$\mathcal{T}(E/E') = \prod_{p \leq \infty} \mathcal{T}_p(E/E'), \quad \text{where } \mathcal{T}_p(E/E') = \tfrac{1}{2}|H^1_\phi(\mathbb{Q}_p, \ker\phi)|.$$

Theorem 3.6 (Dokchitser and Dokchitser [9, Lemmas 4.2 and 4.3]). *For $p \neq 2$ finite*,

$$\tfrac{1}{2}|H^1_\phi(\mathbb{Q}_p, \ker\phi)| = \frac{c_p(E')}{c_p(E)}.$$

4. Computing ranks

4A. ***Enumerating curves.*** We produce a list of all isomorphism classes in $\mathcal{F}$ up to height N by computing the Farey sequence of order N to get a list of (a, b), where a and b are coprime and have opposite parities. Each pair (a, b) gives a curve in $\mathcal{F}$ of minimal height in its isomorphism class. This gives us 202,462 ordered isomorphism classes of $(2, 8)$-torsion curves with height less than 1000.

4B. ***Procedure.*** To make our rank computations feasible, we assume two standard conjectures: the Birch and Swinnerton-Dyer conjecture (BSD) and the generalized Riemann hypothesis (GRH). BSD allows us to obtain an upper bound of the rank by computing the analytic rank numerically. GRH provides the conjecturally best bound for the error term of the L-function attached to an elliptic curve, which improves the efficiency of the analytic rank computation. An immediate consequence of the BSD conjecture is the parity conjecture, which states that the root number agrees with the parity of the rank. This allows us to determine the rank when the upper bound and lower bound we calculated for the rank differ by 1.

We computed the rank using a combination of Sage and Magma [6]. We first ran Cremona's `mwrank` in Sage, which carries out 2-descent and searches for rational points with low height. This function gave us an upper bound and a lower bound for the rank of each curve in our database. If the bounds agreed, this determined the rank. If the bounds differed by 1, the rank was obtained conditional on the parity conjecture. This process determined the rank of 52.1% of the curves.

If the rank was not determined at this stage, we ran the Sage function `analytic_rank_upper_bound`, which computes an upper bound on the analytic rank conditional on GRH and takes a parameter Δ, using Bober's method in [5]. The runtime is exponential in Δ, but a higher Δ potentially gives a better bound. We ran the function repeatedly with increasing values of Δ up to at most 2.0, or until the rank's upper bound differed from the lower bound by at most 1. After this stage, we still had 44.2% curves with unknown rank.

Because of the large number of curves remaining, it was computationally unfeasible to run with higher Δ for all of them. Restricting to curves with $H < 100$, only 153 remained at this stage, and we were able to continue the process up to $\Delta = 3.8$. After this, only 15 curves were left with $H < 100$. Computing the analytic rank becomes more difficult as the conductor increases. Since the parameter height appears

to be positively correlated with the conductor, as is seen in Figure 1, it became more and more difficult to determine the rank the further we got along.

A recent implementation of Fisher's `TwoPowerIsogenyDescentRankBound` [11] in Magma is faster and a better fit for our purposes since our curves have full rational 2-torsion. Using this, we were able to determine the ranks of more than 90% of the curves up to $H < 1000$.

For the remaining curves, we returned to Sage. We ran analytic rank with higher values of Δ, up to at least 3.2, and did a further point search using a higher bound in the `mwrank` function `two_descent`. Altogether, the rank of 40.8% of the curves in our database was determined purely via descent, hence unconditionally.

Initially there was one curve left with $H < 100$: this is the curve with parameter $t = \frac{66}{97}$. Thanks to Klagsbrun for suggesting the use of `AnalyticRank` in Magma, we were able to show that this curve has rank 0. The ranks of all curves with $H < 100$ were determined, conditional on GRH and BSD.

The list of high rank curves maintained by Dujella [10] contains 28 rank-3 curves, of which 26 have $H < 1000$. Our computations recovered the rank of 17 of them. The rank of the remaining nine curves, which were all discovered by Fisher, were included in our database for completeness. In addition to the list, we found an extra rank-3 curve at $t = \frac{9}{296}$.

5. Results and analysis of computed data

5A. ***Rank.*** In the $(2, 8)$-torsion family, we very quickly observe a possible turnaround point in average rank. The average rank seems to peak at $H = 24$ with value 0.744, after 121 curves are computed, then steadily decreases to 0.626 at $H = 99$. See Figure 2.

Looking at all curves with $H < 1000$, the behaviour is less certain because of the number of curves with undetermined ranks: we are only able to compute the rank of 186,876 curves, which is 92.3%. For the remaining curves, we have upper bounds and lower bounds from our computations. None of these upper bounds is greater than 3, so no rank-4 curve can exist with $H < 1000$. In Figure 3, we plot the computed upper and lower bounds for the average rank.

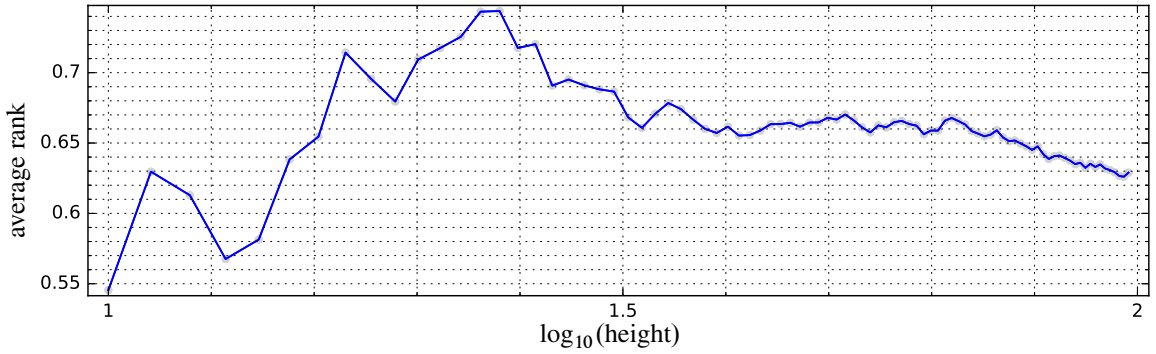


Figure 2. Average rank up to height 100 in the $(2, 8)$-torsion family.

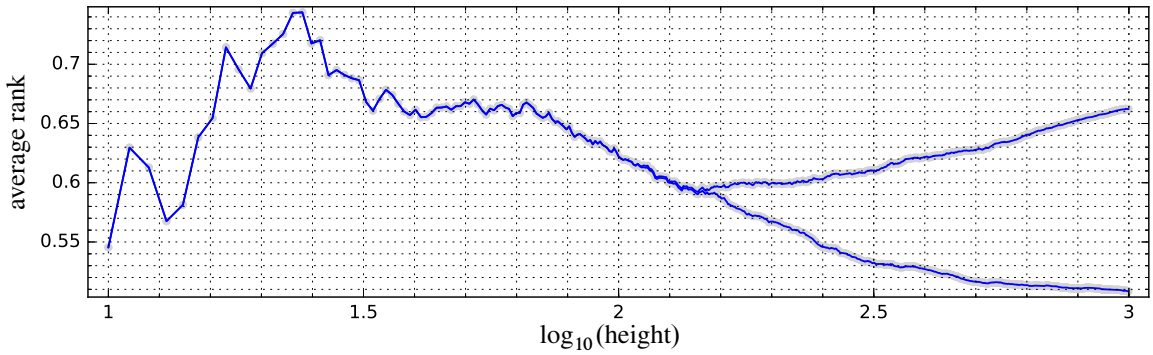


Figure 3. Average rank up to height 1000 in the $(2,8)$-torsion family.

rank	$H<100$	(%)	$H<250$	(%)	$H<500$	(%)	$H<1000$	(%)
0	865	(43.3)	5689	(45.1)	22160	(43.8)	84763	(41.9)
1	1021	(51.1)	6243	(49.5)	25110	(49.7)	101432	(50.1)
2	111	(5.6)	307	(2.4)	465	(0.9)	652	(0.3)
3	3	(0.2)	10	(0.1)	24	(0.0)	27	(0.0)
≥ 4	0	(0.0)	0	(0.0)	0	(0.0)	0	(0.0)
unknown	0	(0.0)	358	(2.8)	2806	(5.5)	15585	(7.7)
total	2000	(100.0)	12607	(100.0)	50565	(100.0)	202461	(100.0)
average	0.626		[0.546, 0.604]		[0.516, 0.628]		[0.508,0.663]	

Table 1. Rank distribution up to different heights.

5B. ***Size of the* 2*-Selmer group.*** To get a clearer picture of the behaviour of the average size of the 2-Selmer group, we computed data beyond height 1000, and it seems to be divergent (see Figure 4). In Section 6B, we prove that this is indeed the case.

5C. ***Tamagawa product.*** The average Tamagawa product in the $(2,8)$-torsion family also behaves differently from the one in [1]. In their data, the average Tamagawa product peaks at 1.84 at naive

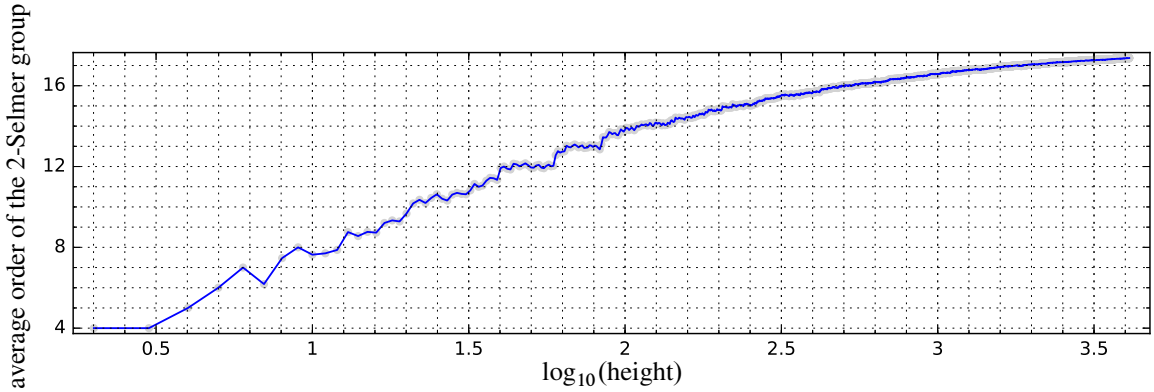


Figure 4. Average size of the 2-Selmer group in the $(2,8)$-torsion family.

rank $\mathrm{Sel}_2(E)$	$H<100$ (%)	$H<1000$ (%)	$H<2000$ (%)	$H<4000$ (%)
2	346 (17.3)	29943 (14.8)	117397 (14.5)	462688 (14.3)
3	799 (40.0)	70856 (35.0)	278930 (34.4)	1107482 (34.2)
4	586 (29.3)	62903 (31.1)	252357 (31.1)	1009839 (31.2)
5	222 (11.1)	29287 (14.5)	120373 (14.9)	487277 (15.0)
6	44 (2.2)	7934 (3.9)	34104 (4.2)	142043 (4.4)
7	3 (0.2)	1386 (0.7)	6329 (0.8)	27823 (0.9)
8	0 (0.0)	147 (0.1)	811 (0.1)	3743 (0.1)
9	0 (0.0)	5 (0.0)	51 (0.0)	333 (0.0)
10	0 (0.0)	0 (0.0)	3 (0.0)	28 (0.0)
≥ 11	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
total	2000 (100)	202461 (100)	810352 (100)	3241228 (100)
average $\lvert \mathrm{Sel}_2(E) \rvert$	13.728	16.574	17.055	17.361

Table 2. 2-Selmer rank distribution up to different heights.

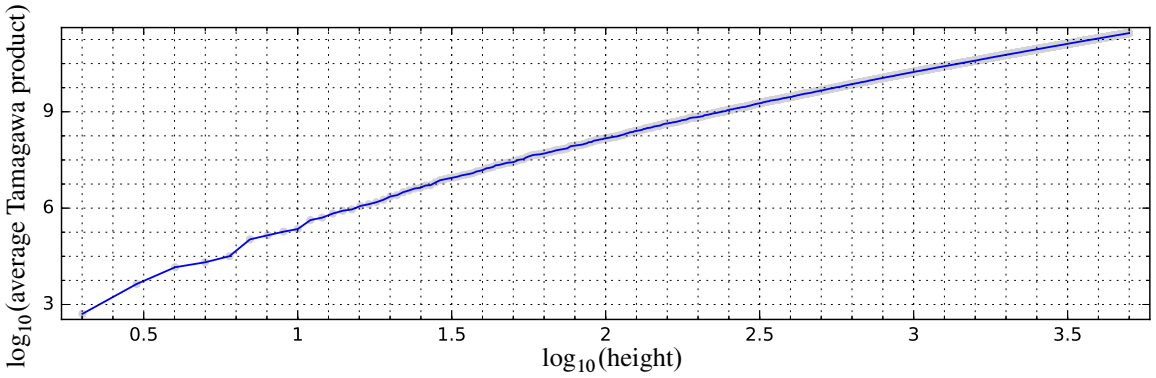


Figure 5. Average Tamagawa product in $\log_{10}$ scale in the $(2,8)$-torsion family.

root number	$H<100$ (%)	$H<1000$ (%)	$H<10000$ (%)
1	976 (48.8)	100927 (49.9)	10125245 (50.0)
-1	1024 (51.2)	101534 (50.1)	10136574 (50.0)
total	2000 (100)	202461 (100)	20261819 (100)
average	-0.024000	-0.002998	-0.000559

Table 3. Root number distribution up to different heights.

height $6.3 \cdot 10^5$, then decreases with respect to the naive height. However in Figure 5, we see that it is increasing in the $(2,8)$-torsion family, and that its value is much larger than 1.84. In Section 6A, we show that the average Tamagawa product is unbounded for this family.

5D. ***Root number.*** The average root number appears to converge to 0, as shown in Figure 6.

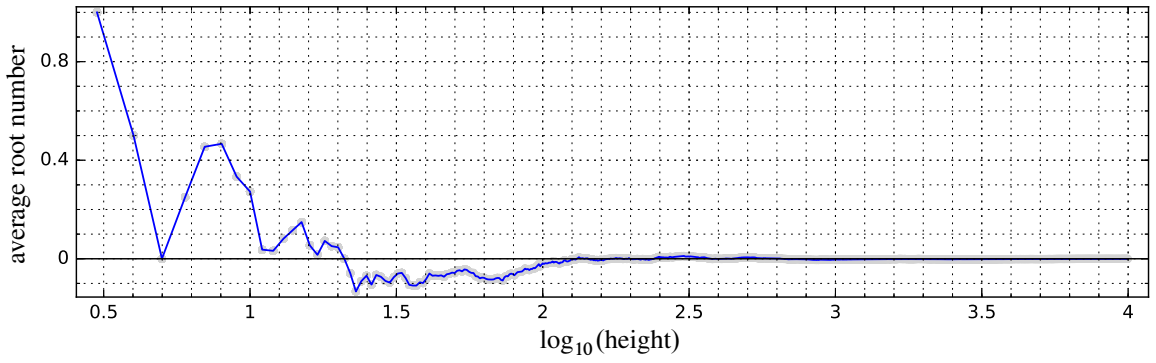


Figure 6. Average root number in the $(2,8)$-torsion family.

6. Proofs

6A. ***The average Tamagawa product is unbounded.*** To find the numbers $c_p(E)$, we apply Tate's algorithm [18]. We look at the model

$$E : y^2 - xy = x^3 + \tfrac{1}{4}(S^4 + T^4 - 1)x^2 + \tfrac{1}{16}S^4T^4x,$$

where $S = 2ab$ and $T = b^2 - a^2$. Again a and b are coprime and have opposite parities. The discriminant of E is $\Delta_E = \frac{1}{2^8}S^8T^8(T^4 - S^4)^2$. Note that S, T and $(T^4 - S^4)^2$ are pairwise coprime. By Tate's algorithm [18], we get

$$c_p = \begin{cases} v_p(\Delta_E) & \text{if } p \mid ST \text{ or } \left(p \mid T^4 - S^4 \text{ and } \left(\frac{-1}{p}\right) = 1\right), \\ 2 & \text{if } p \mid T^4 - S^4 \text{ and } \left(\frac{-1}{p}\right) = -1, \\ 1 & \text{otherwise.} \end{cases}$$

Combining the local factors $c_p(E)$, we get

$$\mathcal{T}(E) = \prod_p c_p(E) = \prod_{\substack{p \mid T^4 - S^4 \\ \left(\frac{-1}{p}\right) = -1}} 2 \prod_{\substack{p^k \parallel (T^4 - S^4)^2 \\ \left(\frac{-1}{p}\right) = 1}} k \prod_{p^l \parallel \frac{1}{2^8}S^8T^8} l.$$

Theorem 6.1. *The average Tamagawa product in the* $(2,8)$*-torsion family up to height* N *has order of magnitude* $(\log N)^{33}$.

Proof. We estimate the sum

$$S(N) := \sum_{\substack{a,b \le N, 2 \mid a \\ (a,b) = 1}} \prod_{\substack{p \mid T^4 - S^4 \\ \left(\frac{-1}{p}\right) = -1}} 2 \prod_{\substack{p^k \parallel (T^4 - S^4)^2 \\ \left(\frac{-1}{p}\right) = 1}} k \prod_{p^l \parallel \frac{1}{2^8}S^8T^8} l.$$

Let $H_1(a,b) = (a^2 - b^2 - 2ab)(a^2 - b^2 + 2ab)$, $H_2(a,b) = a^2 + b^2$ and $H_3(a,b) = ab(b-a)(b+a)$. Note that the factors $a^2 - b^2 - 2ab$, $a^2 - b^2 + 2ab$, $a^2 + b^2$, a, b, $b - a$, $b + a$ are pairwise coprime.

Let

$$f(H)=\prod_{\substack{p\mid H\\ (\frac{-1}{p})=-1}} 2\prod_{\substack{p^k\parallel H\\ (\frac{-1}{p})=1}} k \quad\text{and}\quad g(H)=\prod_{p^l\parallel H} l.$$

Let $P^+(x)$ and $P^-(x)$ denote the largest and smallest prime divisor of x respectively. Fix $\epsilon>0$. Factorize $H_i(a,b)$ into d_i and $H_i(a,b)/d_i$, so that $P^-(d_i)<N^\epsilon$, and $P^+(H_i(a,b)/d_i)\geq N^\epsilon$. Then $\max_{a,b\leq N}\{H_1(a,b)^2H_2(a,b)^4, H_3(a,b)^8\}\leq N^{32}$, so $H_1(a,b)^2H_2(a,b)^4$ and $H_3(a,b)^8$ each have at most $32/\epsilon$ prime factors greater than N^ϵ. Therefore $f(d_1^2d_2^4)\leq f(H_1(a,b)^2H_2(a,b)^4)\ll_\epsilon f(d_1^2d_2^4)$. Similarly $g(d_3^8)\leq g(H_3(a,b)^8)\ll_\epsilon g(d_3^8)$. We have

$$\begin{aligned}S(N)&=\sum_{\substack{a,b\leq N,2\mid a\\ (a,b)=1}} f(H_1(a,b)^2H_2(a,b)^4)g(H_3(a,b)^8)\\ &\asymp \sum_{\substack{d_1,d_2,d_3\\ P^+(d_i)<N^\epsilon}} f(d_1^2d_2^4)g(d_3^8)\sum_{\substack{a,b\leq N,\ 2\mid a,\ (a,b)=1\\ d_i\mid H_i(a,b)\\ P^-(H_i(a,b)/d_i)\geq N^\epsilon}} 1.\end{aligned}$$

Write $a=\alpha+ud_1d_2d_3$ and $b=\beta+vd_1d_2d_3$. Since H_1, H_2 and H_3 are pairwise coprime, we only need to look at coprime d_1, d_2 and d_3. Since H_1, H_2 are odd and H_3 is even, we consider only odd d_1, d_2 and even d_3. Note that $a,b\mid H_3(a,b)$ by construction. Suppose $p\mid(a,b)$; then $p\mid d_2$ or $p>N^\epsilon$. We have

$$\sum_{\substack{a,b\leq N\\ \exists p\geq N^\epsilon:\ p\mid(a,b)}} 1=O\Big(\sum_{p\geq N^\epsilon}\Big(\frac{N}{p}\Big)^2\Big)=O(N^{2-\epsilon}).$$

We can exclude pairs of a and b with $P^-((a,b))>N^\epsilon$ with a cost of $O(N^{2-\epsilon})$.

$$\sum_{\substack{a,b\leq N,\ 2\mid a,\ (a,b)=1\\ d_i\mid H_i(a,b)\\ P^-(H_i(a,b)/d_i)\geq N^\epsilon}} 1=\sum_{\substack{\alpha,\beta<d_1d_2d_3\\ 2\mid\alpha,\ d_i\mid H_i(\alpha,\beta)\\ p\mid d_1d_2d_3\Rightarrow(p\nmid\beta\text{ or }p\nmid\alpha)}}\ \sum_{\substack{u,v<N/(d_1d_2d_3)\\ P^-(H_i(a,b)/d_i)\geq N^\epsilon}} 1+O(N^{2-\epsilon}).$$

By the small sieve [14, Theorem 2.6, p. 85] we have

$$\sum_{\substack{u,v<N/(d_1d_2d_3)\\ P^-(H_i(a,b)/d_i)\geq N^\epsilon}} 1\asymp\frac{N^2}{d_1^2d_2^2d_3^2}\prod_{p<N^\epsilon}\Big(1-\frac{7+\left(\frac{-1}{p}\right)+2\cdot\left(\frac{2}{p}\right)}{p}\Big)\asymp\frac{N^2}{d_1^2d_2^2d_3^2(\log N)^7}.$$

It remains to compute

$$\sum_{\substack{\alpha,\beta<d_1d_2d_3\\ 2\mid\alpha,\ d_i\mid H_i(\alpha,\beta)\\ p\mid d_1d_2d_3\Rightarrow(p\nmid\beta\text{ or }p\nmid\alpha)}} 1=\sum_{\substack{\alpha,\beta<d_1\\ d_1\mid H_1(\alpha,\beta)\\ p\mid d_1\Rightarrow(p\nmid\beta\text{ or }p\nmid\alpha)}} 1\ \sum_{\substack{\alpha,\beta<d_2\\ d_2\mid H_2(\alpha,\beta)\\ p\mid d_2\Rightarrow(p\nmid\beta\text{ or }p\nmid\alpha)}} 1\ \sum_{\substack{\alpha,\beta<d_3\\ 2\mid\alpha,\ d_3\mid H_3(\alpha,\beta)\\ p\mid d_3\Rightarrow(p\nmid\beta\text{ or }p\nmid\alpha)}} 1.$$

By the Chinese remainder theorem, it suffices to count the number of solutions of H_i modulo $p^v \| d_i$ for each prime p dividing d_i. We have

$$h_1(p^v) := \sum_{\substack{\alpha,\beta<p^v \\ p^v \mid H_1(\alpha,\beta) \\ p\nmid\beta \text{ or } p\nmid\alpha}} 1 = \begin{cases} 4\phi(p^v) & \text{if 2 is a square modulo } p^v, \\ 0 & \text{otherwise;} \end{cases}$$

$$h_2(p^v) := \sum_{\substack{\alpha,\beta<p^v \\ p^v \mid H_2(\alpha,\beta) \\ p\nmid\beta \text{ or } p\nmid\alpha}} 1 = \begin{cases} 2\phi(p^v) & \text{if } -1 \text{ is a square modulo } p^v, \\ 0 & \text{otherwise;} \end{cases}$$

$$h_3(p^v) := \sum_{\substack{\alpha,\beta<p^v \\ p^v \mid H_3(\alpha,\beta) \\ p\nmid\beta \text{ or } p\nmid\alpha}} 1 = \begin{cases} 4\phi(p^v) & \text{if } p \neq 2, \\ \phi(p^v) & \text{if } p = 2. \end{cases}$$

We extend h_1, h_2 and h_3 to multiplicative functions. Then the sum becomes

$$\begin{aligned} S(N) &\asymp \frac{N^2}{(\log N)^7} \sum_{\substack{d_1,d_2,d_3 \\ P^+(d_i)<N^\epsilon}} \frac{f(d_1^2d_2^4)g(d_3^8)h_1(d_1)h_2(d_2)h_3(d_3)}{d_1^2d_2^2d_3^2} \\ &\asymp \frac{N^2}{(\log N)^7} \prod_{p<N^\epsilon} \left(1+\frac{f(p^2)h_1(p)}{p^2}\right)\left(1+\frac{f(p^4)h_2(p)}{p^2}\right)\left(1+\frac{g(p^8)h_3(p)}{p^2}\right) \\ &\asymp \frac{N^2}{(\log N)^7} \prod_{p<N^\epsilon} \left(1+\frac{1}{p}\right)^4\left(1+\frac{1}{p}\right)^4\left(1+\frac{1}{p}\right)^{32} \asymp N^2(\log N)^{33}. \end{aligned}$$

The total number of curves up to height N has order of magnitude N^2 as discussed in Section 2A. Therefore the average Tamagawa product is of the size $(\log N)^{33}$. □

6B. ***The average size of the* 2*-Selmer group is unbounded.*** We follow the approach in [15] to show the average Tamagawa ratio diverges in the $(2, 8)$-torsion family, which implies that the average size of the 2-Selmer group is unbounded.

The curve obtained by the degree-2 isogeny $\phi : E \to E'$ corresponding to the rational subgroup generated by the point $(0, 0)$ is

$$E' : y^2 - xy = x^3 + \tfrac{1}{4}((S^2+T^2)^2 + 4S^2T^2 - 1)x^2 + \tfrac{1}{4}(S^2T^2(S^2+T^2)^2)x,$$

which has discriminant $\Delta_{E'} = \frac{1}{2^4}S^4T^4(T^4-S^4)^4$. Using Tate's algorithm and looking at Table 1 in [9], we find that the Tamagawa ratio for any finite prime p is

$$\mathcal{T}_p(E/E') = \frac{c_p(E')}{c_p(E)} = \begin{cases} 2 & \text{if } p \mid S^4 - T^4 \text{ and } \left(\frac{-1}{p}\right) = 1, \\ \frac{1}{2} & \text{if } p \mid ST, \\ 1 & \text{otherwise.} \end{cases}$$

Since the discriminants Δ_E and Δ'_E are both positive, we have $\mathcal{T}_\infty(E/E') = 1$.

Theorem 6.2. *The logarithmic Tamagawa ratio* $t(a,b) := \log_2 \mathcal{T}(E/E')$ *tends to a normal distribution with mean* $-2\log\log N + O(1)$ *and variance* $6\log\log N + O(1)$.

Before we turn to the proof, let us look at the application of Theorem 6.2. We find that $t(a,b)\log 2$ tends to a normal distribution with mean μ and variance σ^2 given by

$$\mu := -2(\log 2)(\log\log N) + O(1), \quad \sigma^2 := 6(\log 2)^2 \log\log N + O(1).$$

Hence $\mathcal{T}(E/E') = \exp(t(a,b)\log 2)$ tends to a log-normal distribution which has mean $\exp\big(\mu + \frac{1}{2}\sigma^2\big) = e^{O(1)}(\log N)^{(3\log 2 - 2)\log 2}$. Since $3\log 2 - 2 > 0$, the mean increases as N increases. From the discussion in Section 3C, we know that $|\operatorname{Sel}_2(E)| \geq |\operatorname{Sel}_\phi(E)| \geq \mathcal{T}(E/E')$, so the following theorem is a corollary of Theorem 6.2.

Theorem 6.3. *The average size of the* 2*-Selmer group tends to infinity in the* $(2,8)$*-torsion family.*

Proof of Theorem 6.2. Let $H_1 = (a^2 - b^2 - 2ab)(a^2 - b^2 + 2ab)(a^2 + b^2)$ and $H_2 = ab(b-a)(b+a)$. Throughout this proof, we will assume p is an odd prime as the contribution of the prime 2 can be taken into the error term. Define

$$f_p(H) := \mathbb{1}_{p \mid H} \cdot \mathbb{1}_{\left(\frac{-1}{p}\right)=1} \quad \text{and} \quad g_p(H) := \mathbb{1}_{p \mid H},$$

where $\mathbb{1}$ denotes the indicator function. Then

$$t(a,b) = f(H_1(a,b)) - g(H_2(a,b)), \quad \text{where } f(H) := \sum_p f_p(H) \text{ and } g(H) := \sum_p g_p(H).$$

For any function F and any property $\mathcal{P}$ defined on the set

$$\mathcal{A}_N := \{(a,b) : a, b \leq N,\ a \text{ and } b \text{ coprime and have opposite parities}\},$$

define

$$\mathbb{P}_N(\mathcal{P}) = \frac{\sum_{(a,b)\in\mathcal{A}_N} \mathbb{1}_{\mathcal{P}(a,b)}}{|\mathcal{A}_N|} \quad \text{and} \quad \mathbb{E}_N(F) = \frac{\sum_{(a,b)\in\mathcal{A}_N} F(a,b)}{|\mathcal{A}_N|}.$$

Fix $\epsilon > 0$. For $p \leq N^\epsilon$, by counting the number of solutions of H_1, H_2 modulo p,

$$\mathbb{E}_N(f_p(H_1)) = \mathbb{P}_N(H_1 \equiv 0 \bmod p) = \begin{cases} \frac{6}{p+1} + O\big(\frac{1}{N^{2(1-\epsilon)}}\big) & \text{if } \big(\frac{2}{p}\big) = \big(\frac{-1}{p}\big) = 1, \\ \frac{2}{p+1} + O\big(\frac{1}{N^{2(1-\epsilon)}}\big) & \text{if } \big(\frac{2}{p}\big) = -1,\ \big(\frac{-1}{p}\big) = 1; \end{cases}$$

$$\mathbb{E}_N(g_p(H_2)) = \mathbb{P}_N(H_2 \equiv 0 \bmod p) = \tfrac{4}{p+1} + O\big(\tfrac{1}{N^{2(1-\epsilon)}}\big).$$

Since $\max_{a,b\leq N}\{|H_1(a,b)|, |H_2(a,b)|\} \leq N^6$, each of H_1 and H_2 can only be divisible by at most $6/\epsilon$ prime factors larger than N^ϵ, so $\sum_{p>N^\epsilon} f_p(H_1)$ and $\sum_{p>N^\epsilon} g_p(H_2)$ are bounded above by $6/\epsilon$. Let $F(N) := \sum_{p\leq N^\epsilon} f_p(H_1)$ and $G(N) := \sum_{p\leq N^\epsilon} g_p(H_2)$. Then $F(N) = f(H) + O(1)$ and $G(N) = g(H) + O(1)$ for $(a,b) \in \mathcal{A}_N$.

We define the following random variables to model $f_p(H_1)$ and $g_p(H_2)$:

$$X_p = \begin{cases} 1 & \text{with probability } \frac{2}{p+1}\left(2+\left(\frac{2}{p}\right)\right), \\ 0 & \text{with probability } 1-\frac{2}{p+1}\left(2+\left(\frac{2}{p}\right)\right) \end{cases} \quad \text{if } \left(\tfrac{-1}{p}\right)=1,$$

$$Y_p = \begin{cases} 1 & \text{with probability } \frac{4}{p+1}, \\ 0 & \text{with probability } 1-\frac{4}{p+1}, \end{cases}$$

so that $\{X_p\}_p \cup \{Y_p\}_p$ are independent except $\mathbb{P}(X_p = 1 \text{ and } Y_p = 1) = 0$. If $\left(\frac{-1}{p}\right) \neq 1$, then $X_p = 0$ with probability 1. Let $X(N) = \sum_{p \leq N^\epsilon} X_p$ and $Y(N) = \sum_{p \leq N^\epsilon} Y_p$. By the multidimensional central limit theorem, $X(N)$ and $Y(N)$ converge to independent normal distributions as $N \to \infty$. Note that $X(N)$ has mean and variance $2\log\log N + O(1)$; $Y(N)$ has mean and variance $4\log\log N + O(1)$.

Since mixed moments determine the multinomial distribution, we want to show that the mixed moments of $F(N)$ and $G(N)$ converge to those of $X(N)$ and $Y(N)$. We have by construction

$$\begin{aligned}\mathbb{E}_N(F(N)^k G(N)^l) &= \sum_{\substack{p_1,\dots,p_k \leq N^\epsilon \\ q_1,\dots,q_l \leq N^\epsilon}} \mathbb{P}_N(H_1 \equiv 0 \bmod p_i \text{ and } H_2 \equiv 0 \bmod q_j) \\ &= \mathbb{E}(X(N)^k Y(N)^l) + O\left(\frac{(4\log\log N)^{k+l-1}}{N^{2(1-\epsilon)}}\right).\end{aligned}$$

From this we compute

$$\begin{aligned}&\mathbb{E}_N\big((F(N)-\mathbb{E}_N(F(N)))^k (G(N)-\mathbb{E}_N(G(N)))^l\big) \\ &\qquad = \mathbb{E}\big((X(N)-\mathbb{E}(X(N)))^k (Y(N)-\mathbb{E}(Y(N)))^l\big) + O\left(\frac{(4\log\log N)^{k+l-1}}{N^{2(1-\epsilon)}}\right).\end{aligned}$$

This shows that the distributions of $F(N)$ and $G(N)$ tend to those of $X(N)$ and $Y(N)$ respectively. The difference of two normal distribution is a normal distribution; hence $f(H_1) - g(H_2) = F(N) - G(N) + O(1)$ tends to a normal distribution with mean and variance as claimed. □

Acknowledgements

The authors would like to thank Jennifer Balakrishnan for suggesting the topic and the guidance through the work. We would like to thank Andrew Booker, Jordan Ellenberg, Tom Fisher, Andrew Granville, Wei Ho, Bartosz Naskręcki, Harald Schilly, Jeroen Sijsling, William Stein, Gonzalo Tornaría and John Voight for their advice and help. The authors are indebted to Zev Klagsbrun for the rank computation of the curve with parameter $t = \frac{66}{97}$. The authors thank the organizers of the "Curves and L-functions" summer school held at ICTP in 2017, where this project began: Tim Dokchitser, Vladimir Dokchitser, and Fernando Rodriguez Villegas. We used the open-source software SageMath and CoCalc extensively throughout this project. Chan was supported by the European Research Council grant agreement no. 670239. Hanselman was supported by the research grant 7635.521(16) of the Science Ministry of Baden-Württemberg.

References

[1] Jennifer S. Balakrishnan, Wei Ho, Nathan Kaplan, Simon Spicer, William Stein, and James Weigandt, *Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks*, LMS J. Comput. Math. **19** (2016), supp. A, pp. 351–370. MR 3540965

[2] Manjul Bhargava and Arul Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, preprint, 2013. arXiv 1312.7859

[3] ———, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242. MR 3272925

[4] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves, II*, J. Reine Angew. Math. **218** (1965), 79–108. MR 0179168

[5] Jonathan W. Bober, *Conditionally bounding analytic ranks of elliptic curves*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., no. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 135–144. MR 3207411

[6] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system, I: The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR 1484478

[7] Terris D. Brooks, Elizabeth A. Fowler, Katherine C. Hastings, D. L. Hiance, and M. A. Zimmerman, *Elliptic curves with torsion subgroup $\mathbb{Z}_2 \times \mathbb{Z}_8$: Does a rank* 4 *curve exist?*, J. Summer Undergrad. Math. Sci. Res. Inst. **2006** (2006).

[8] J. W. S. Cassels, *Arithmetic on curves of genus* 1*, VIII: On conjectures of Birch and Swinnerton–Dyer*, J. Reine Angew. Math. **217** (1965), 180–199. MR 0179169

[9] Tim Dokchitser and Vladimir Dokchitser, *Local invariants of isogenous elliptic curves*, Trans. Amer. Math. Soc. **367** (2015), no. 6, 4339–4358. MR 3324930

[10] Andrej Dujella, *High rank elliptic curves with prescribed torsion*, online database, 2012.

[11] Tom Fisher, *Higher descents on an elliptic curve with a rational 2-torsion point*, Math. Comp. **86** (2017), no. 307, 2493–2518. MR 3647969

[12] Jessica Flores, Kimberly Jones, Anne Rollick, and James Weigandt, *A statistical analysis of* 2*-Selmer groups for elliptic curves with torsion subgroup $\mathbb{Z}_2 \times \mathbb{Z}_8$*, J. Summer Undergrad. Math. Sci. Res. Inst. **2007** (2007).

[13] Dorian Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, (Carbondale 1979), Lecture Notes in Math., no. 751, Springer, 1979, pp. 108–118. MR 564926

[14] H. Halberstam and H.-E. Richert, *Sieve methods*, Lond. Math. Soc. Monographs, no. 4, Academic Press, London, 1974. MR 0424730

[15] Zev Klagsbrun and Robert J. Lemke Oliver, *The distribution of the Tamagawa ratio in the family of elliptic curves with a two-torsion point*, Res. Math. Sci. **1** (2014), art. id. 15. MR 3375649

[16] Bartosz Naskręcki, *Mordell–Weil ranks of families of elliptic curves associated to Pythagorean triples*, Acta Arith. **160** (2013), no. 2, 159–183. MR 3105333

[17] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231. MR 2021618

[18] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV, Lecture Notes in Math., no. 476, Springer, 1975, pp. 33–52. MR 0393039

[19] Arnold Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, Math. Forschungsberichte, no. 15, Deutscher Verlag der Wissen., Berlin, 1963. MR 0220685

Received 28 Feb 2018. Revised 23 Sep 2018.

STEPHANIE CHAN: stephanie.chan.16@ucl.ac.uk
Department of Mathematics, University College London, London, United Kingdom

JEROEN HANSELMAN: jeroen.hanselman@uni-ulm.de
Institute of Pure Mathematics, Ulm University Ulm, Germany

WANLIN LI: wanlin@math.wisc.edu
Department of Mathematics, University of Wisconsin, Madison, WI, United States

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

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

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

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 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational 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 thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine