

Experimental investigations on Lehmer's conjecture for elliptic curves

Sven Cats, John Michael Clark, Charlotte Dombrowsky,
Mar Curc3 Iranzo, Krystal Maughan, and Eli Orvis

ABSTRACT. In this short note, we give a method for computing a non-torsion point of smallest canonical height on a given elliptic curve $E/\mathbb{Q}$ over all number fields of a fixed degree. We then describe data collected using this method, and investigate related conjectures of Lehmer and Lang using these data.

1. Introduction

Let E be an elliptic curve over a number field K . We denote by $\overline{K}$ a fixed algebraic closure of K and by $\hat{h}$ the canonical height function on $E(\overline{K})$. Recall that $\hat{h}(P) = 0$ if and only if P is a torsion point. There is much interest in studying the canonical heights of non-torsion points. In particular, we have the following conjecture, which is known as Lehmer's conjecture because of its analogy with a conjecture of D.H. Lehmer from 1933 [7]. It describes how the smallest possible height of a non-torsion point $P \in E(\overline{K})$ varies with the (minimal) field $K(P)$ over which P is defined.

CONJECTURE 1.1 (Lehmer). *Let*

$$C_E := \inf \left\{ \hat{h}(P) \cdot [K(P) : K] \right\},$$

where the infimum ranges over the non-torsion points $P \in E(\overline{K}) - E(\overline{K})_{\text{tors}}$. Then the constant C_E satisfies $C_E > 0$.

The other primary conjecture describes how the smallest possible height of a non-torsion point $P \in E(\overline{K})$ defined over an extension of a given degree varies with the curve E . Denote by j_E, Δ_E the j -invariant and minimal discriminant of E/K . We write $N_{K/\mathbb{Q}} : K \rightarrow \mathbb{Q}$ for the norm map and see Definition 2.1 for the height function $h : \mathbb{P}^1(\overline{K}) \rightarrow \mathbb{R}_{\geq 0}$. Consider the quantity $M_E = \max\{h(j_E), \log |N_{K/\mathbb{Q}} \Delta_E|, 1\}$.

CONJECTURE 1.2 (Lang). *Let*

$$C_{K,d} := \inf \left\{ \frac{\hat{h}(P)}{M_{E'}} \right\},$$

where the infimum ranges over all elliptic curves E'/K and the non-torsion points $P \in E'(\overline{K}) - E'(\overline{K})_{\text{tors}}$ for which $K(P)$ is contained in a degree d extension of K . Then the constant $C_{K,d}$ satisfies $C_{K,d} > 0$.

Although there is theoretical progress on these conjectures and their generalisations to abelian varieties over number fields, very little experimental work has been done investigating the values of C_E and $C_{K,d}$. In this short paper, we describe a database of quadratic points of small height on 17,834 elliptic curves over the rationals $K = \mathbb{Q}$. In 728 of the cases, the point in the database is provably the point of smallest height on the given elliptic curve over any quadratic field. The computations to collect our data required just over 800 hours of CPU time. We use these data to investigate the constants in Conjectures 1.1 and 1.2.

We proceed first with a brief background on heights, followed by a description of the theoretical results underlying the algorithm used to build our database. We then discuss some preliminary observations about the resulting data, and possible future work.

2. Computing minimal heights over field extensions

Let K be a number field with fixed algebraic closure $\overline{K}$, and let E be an elliptic curve over K , given by an affine Weierstrass equation with coefficients in K .

DEFINITION 2.1. Let $x : E(\overline{K}) \rightarrow \mathbb{P}^1(\overline{K})$ denote the map taking the x -coordinate and $h : \mathbb{P}^1(\overline{K}) \rightarrow \mathbb{R}_{\geq 0}$ the (absolute logarithmic) Weil height on $\mathbb{P}^1(\overline{K})$, as defined in [6], Section B.2. By a standard abuse of notation, we also denote by $h : E(\overline{K}) \rightarrow \mathbb{R}_{\geq 0}$ the map defined by $P \mapsto h(x(P))$. We denote the canonical height on E/K by

$$\hat{h} : E(\overline{K}) \rightarrow \mathbb{R}_{\geq 0}, \quad P \mapsto \lim_{n \rightarrow \infty} \frac{1}{4^n} h(2^n P).$$

Recall that the canonical height is the unique quadratic form $E(\overline{K}) \rightarrow \mathbb{R}_{\geq 0}$ with the property that the function $P \mapsto |h(P) - \hat{h}(P)|$ is bounded.

Let E be an elliptic curve over a number field K and let $\mathcal{F}$ be a set of finite field extensions of K with the following properties:

- If $F \in \mathcal{F}$ and $F' \subset F$, then $F' \in \mathcal{F}$.
- The set of degrees $\{[F : K] : F \in \mathcal{F}\}$ is finite.

Consider the infimum

$$C_{E,\mathcal{F}} := \inf_{F \in \mathcal{F}, P \in E(F) - E(F)_{\text{tors}}} \left\{ \hat{h}(P) \cdot [F : K] \right\}.$$

REMARK 2.2. The first property ensures that whenever $F \in \mathcal{F}$ and $P \in E(F)$, the set $\mathcal{F}$ also contains the minimal field of definition $K(P)$ of P . The second property ensures that the subset of number fields in $\mathcal{F}$ of discriminant bounded by a given value is finite. In turn, using (for example) Lemma 2.3 below, this implies that a Northcott property holds for all fields in $\mathcal{F}$: There are finitely many points of bounded height on E over fields in $\mathcal{F}$. Thus the minimum height of such points exists and it follows that $C_{E,\mathcal{F}} > 0$. The fact that $C_{E,\mathcal{F}} > 0$ also follows directly from Theorem 2.4 and it is predicted by Conjecture 1.1 since $C_{E,\mathcal{F}} \geq C_E$.

In this section we explain how to explicitly compute $C_{E,\mathcal{F}}$ using a lower bound on the Weil height $h(P)$ of the x -coordinate, and an upper bound on the difference $|h(P) - \hat{h}(P)|$ with the canonical height.

We proceed in two steps: First we determine a finite set $\mathcal{F}' \subset \mathcal{F}$ such that $C_{E,\mathcal{F}'} = C_{E,\mathcal{F}}$. Then we explain how to solve the finite problem of determining $C_{E,\mathcal{F}'}$. Computational challenges arise when $\mathcal{F}'$ is large; we discuss these in the next section, where we consider the case $K = \mathbb{Q}$ and $\mathcal{F} = \{F/\mathbb{Q} : [F : \mathbb{Q}] \leq 2\}$.

As noted under Definition 2.1, we can fix $B_E \in \mathbb{R}_{>0}$ such that

$$(1) \quad |h(P) - \hat{h}(P)| \leq B_E$$

for all $P \in \cup_{F \in \mathcal{F}} E(F)$, see for example [10] for an explicit value of B_E . For now, any B_E satisfying (1) will do, but for our explicit computations it is useful to have B_E as small as possible. We will use a modified version of the bound given in [3], which we describe in Section 2.1.

LEMMA 2.3. *Let $D \in \mathbb{R}_{\geq 0}$, $F \in \mathcal{F}$, and $d = [F : K]$. Let δ_K be the number of Archimedean places of K . Define $\Delta(D, E, F) \in \mathbb{R}_{>0}$ by*

$$\Delta(D, E, F) := \exp(d\delta_K \log d + d(2d - 2)B_E + (2d - 2)D).$$

If the discriminant Δ_F of F satisfies $|\Delta_F| \geq \Delta(D, E, F)$, then $\hat{h}(P) \geq \frac{D}{d}$ for all $P \in E(F) - E(F)_{\text{tors}}$ satisfying $K(P) = F$. Further, if $[F : K] = [F' : K]$, then $\Delta(D, E, F) = \Delta(D, E, F')$.

PROOF. By Theorem 2 in [9] we have $h(P) \geq \frac{1}{2d-2} \left(\frac{1}{d} \log |\Delta_F| - \delta_K \log d \right)$. The first part of the lemma follows by combining $|\Delta_F| \geq \Delta(D, E, F)$ and Equation (1). The second part of the lemma is clear from the definition of $\Delta(D, E, F)$. $\square$

We can now reduce $\mathcal{F}$ to a finite set.

THEOREM 2.4. *Let $D' \in \mathbb{R}_{\geq 0}$ be such that $C_{E,\mathcal{F}} \leq D'$ and*

$$\mathcal{F}' = \{F \in \mathcal{F} : |\Delta_F| \leq \Delta(D', E, F)\}.$$

Then, $\mathcal{F}'$ is finite and $C_{E,\mathcal{F}'} = C_{E,\mathcal{F}}$.

PROOF. By our initial assumptions on $\mathcal{F}$, the set $\{[F : K] : F \in \mathcal{F}\}$ is finite. Therefore, it follows from the second part of Lemma 2.3 that the maximum $\Delta = \max\{\Delta(D', E, F) : F \in \mathcal{F}\}$ exists. The set $\mathcal{F}_\Delta = \{F \in \mathcal{F} : |\Delta_F| \leq \Delta\}$ is finite by the Hermite–Minkowski Theorem, and hence its subset $\mathcal{F}' \subset \mathcal{F}_\Delta$ is also finite. The first part of Lemma 2.3 implies that $C_{E,\mathcal{F}'} = C_{E,\mathcal{F}}$. $\square$

In principle, we can therefore compute $C_{E,\mathcal{F}}$ as follows: Do an initial search to find $F' \in \mathcal{F}, P' \in E(F')$ with $K(P') = F'$ such that $D' = \hat{h}(P')[F' : K]$ is small. Then $C_{E,\mathcal{F}} \leq D'$ and we write $\mathcal{F}' \subset \mathcal{F}$ for the associated finite set of fields from Theorem 2.4. In theory any F', P' work, but in practice it is worth spending more time in the initial search, as a smaller D' decreases the number of fields in $\mathcal{F}'$ to be considered later. For each $F \in \mathcal{F}'$ do a finite search to find the points $P \in E(F)$ such that

$$(2) \quad h(P) \leq \frac{D'}{[F : K]} + B_E.$$

If $\mathcal{F}'$ is not too large¹ and we can list it explicitly, we obtain in this way the finite list of F, P satisfying (2), among which is a number field $F_E \in \mathcal{F}$ and a $P_E \in E(F_E) - E(F_E)_{\text{tors}}$ such that $C_{E, \mathcal{F}} = \hat{h}(P_E) \cdot [F_E : K]$.

2.1. A modified CPS height bound. Let E be an elliptic curve over a number field K and $\mathcal{F}$ a set of extensions of K such that the set of degrees $\{[F : K] : F \in \mathcal{F}\}$ is finite. In this subsection we compute a bound $B_E \in \mathbb{R}_{\geq 0}$ such that $h(P) - \hat{h}(P) \leq B_E$ for all $P \in E(F)$ as F ranges over $\mathcal{F}$. As mentioned, there is previous work (for example Silverman [10] and Bruin [2]) computes a bound on $h(P) - \hat{h}(P)$ for all $P \in E(\bar{K})$, but in practice a smaller bound is desirable. For a given $F \in \mathcal{F}$, Cremona, Prickett and Siksek describe a bound $B_{E, F}$ for $h(P) - \hat{h}(P)$ for all $P \in E(F)$ in Theorem 1 of [3], which is small enough for our purposes, and we now explain how to modify it to work for all $F \in \mathcal{F}$ at once.

Indeed, for $F \in \mathcal{F}$, the bound $B_{E, F}$ is of the form

$$B_{E, F} = \frac{1}{[F : K]} \sum_v M_v,$$

where the sum ranges over the set of archimedean places of F and the set of primes of F for which E/F_v has bad reduction. The M_v are certain local invariants associated to E/F_v . Since the set of degrees $\{[F : K] : F \in \mathcal{F}\}$ is finite, and since there are only finitely many extensions of $\mathbb{R}$ and $\mathbb{Q}_p$ of any given degree, the set $\{B_{E, F} : F \in \mathcal{F}\}$ attains its maximum and we can set $B_E = \max\{B_{E, F} : F \in \mathcal{F}\}$.

REMARK 2.5. We have implemented the above procedure for computing B_E in the case $K = \mathbb{Q}$ and $\mathcal{F} = \{F/\mathbb{Q} : [F : \mathbb{Q}] \leq 2\}$.

3. Computational Results

We implemented the strategy in Section 2 in the case of quadratic fields using MAGMA version 21.2-2[1] and Sagemath version 10.6 [12]. In particular, for every elliptic curve in the Cremona database [8] of conductor at most 3,000, we conducted an initial search to find points of small height. We then calculated a bound $\Delta = \Delta(D', E, F)$ as in Lemma 2.3, using the height bound in Section 2.1 as our B_E , as well as a bound B on the logarithmic height of the points that needed to be searched as in Equation (2). For curves for which $\Delta < 10^5$ and $B < 50$, we searched all possible x -coordinates to obtain provably the smallest point, using the Sagemath implementation of [4]. In order to keep the computations feasible, for curves where either bound exceeded the numbers described above, we searched only over quadratic fields with $|\Delta_K| \leq 1,000$. We believe this choice is sufficient as in the provable cases the point of smallest height was usually found lying in a field with small discriminant. The resulting datasets and the code used to produce them are available at <https://github.com/EliOrvis/LehmersConjectureForECs>. The datasets contain the following fields:

- the Cremona label for the curve;
- the discriminant of the quadratic field over which the point of smallest height over all quadratic fields is defined;
- the coordinates of the point of smallest height over all quadratic fields;
- the height of this point.

¹What this means exactly depends on the efficiency of the used algorithms and the available memory and computing power. See also Section 4.

REMARK 3.1. In view of the abundance of data in the LMFDB on generators of the Mordell-Weil group of the elliptic curves E in our database and of their quadratic twists, it is not necessary to conduct an initial point search to compute the first bound Δ as these can be found in the LMFDB. Similarly, one could use the LMFDB precomputed rational points defined on E itself or one of its quadratic twists to perform the search for points over quadratic fields. Implementing these changes could improve our algorithm. We thank an anonymous referee for this suggestion.

3.1. Description of data. We ran an initial search on 17,834 elliptic curves, which required just over 800 hours of CPU time running on a server operating Red Hat Enterprise Linux 8.10. We were able to then verify that we found the point of smallest height over all quadratic fields for 86 of these curves. For 542 curves, the initial search failed to find a point, and so there is no point for these curves in our dataset. Among the remaining curves, the first curves in our list (ordered by conductor) for which the discriminant bound obtained by the initial search was too big were the curves with Cremona label 11a1 and 11a2, of conductor 11.

Among all curves in our dataset, the smallest height we found was the point (3) $(27, -119, 1)$ on the elliptic curve $y^2 + xy + y = x^3 + x^2 - 2990x + 71147$, which has Cremona label 1470l1, and height $0.0099641079999 \dots$

We note that the point in (3) was also found by Elkies [5], although his normalization of the height makes his value half of ours. At the same time, Taylor found points of much smaller height on elliptic curves defined over quadratic fields [11] in unpublished work. Our methods, however, differ from both of these previous computations, in that we search broadly over elliptic curves by conductor, whereas these prior computations were targeted searches in families of elliptic curves likely to contain points of small height.

We also make some observations about the quadratic fields over which points of smallest height are defined. In our dataset, the point of smallest height that we found was defined over $\mathbb{Q}$ for 2,199 of the elliptic curves. The next most common fields were the two cyclotomic quadratic fields: $\mathbb{Q}(\sqrt{-3})$ with 1,610 elliptic curves and $\mathbb{Q}(\sqrt{-4})$ with 1,191 elliptic curves. This remained consistent when restricting to curves where our point is provably the smallest over any quadratic field: in this case, the most common field was $\mathbb{Q}(\sqrt{-3})$ with 20 curves, followed by $\mathbb{Q}(\sqrt{-4})$ with 14, and then $\mathbb{Q}$ with 11. Finally, we note that among curves where we have provably found the point of smallest height over all quadratic fields, this point always agrees with the point found in our initial search. Thus, we suspect that for many of the remaining curves, the point in our dataset is in fact the smallest over all quadratic fields.

3.2. Remarks on Conjectures 1.1 and 1.2. We conducted some preliminary investigations into Conjectures 1.1 and 1.2 using the data we collected. The resulting charts can be found at <https://github.com/EliOrvis/LehmersConjectureForECs>. Unfortunately, we did not find a discernible relationship between the smallest height point in our dataset and either the conductor or the discriminant of the elliptic curve.

Acknowledgements. We would like to thank our mentors, Nicole Looper and Shiva Chidambaram, for their guidance throughout the project. We would also like to thank Joseph Silverman, for his mentorship, and Andrew Sutherland, for his computational insights. We thank John Voight for referring us to the article [4]. We would like to thank the organizers Serin Hong, Hang Xue, Alina Bucur, Renee Bell, Brandon Levin, Anthony Várilly-Alvarado, Isabel Vogt and David Zureick-Brown of the 2024 Arizona Winter School on Abelian Varieties. Finally, we would like to thank the National Science Foundation and the Clay Mathematics Institute, and the anonymous referees for their helpful feedback.

References

- [1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [2] P. Bruin. Bornes optimales pour la différence entre la hauteur de Weil et la hauteur de Néron-Tate sur les courbes elliptiques sur $\overline{\mathbb{Q}}$. *Acta Arith.*, 160(4):385–397, 2013.
- [3] J. E. Cremona, M. Prickett, and S. Siksek. Height difference bounds for elliptic curves over number fields. *Journal of Number Theory*, 116(1):42–68, 2006.
- [4] John R. Doyle and David Krumm. Computing algebraic numbers of bounded height. *Math. Comp.*, 84(296):2867–2891, 2015.
- [5] N. Elkies. Nontorsion points of low height on elliptic curves over $\mathbb{Q}$. Available online at: https://people.math.harvard.edu/~elkies/low_height.html, last accessed on 27.05.2025.
- [6] M. Hindry and J. H. Silverman. *Diophantine Geometry*. Springer-Verlag, New York, 2000. An Introduction.
- [7] D. H. Lehmer. Factorization of certain cyclotomic functions. *Ann. of Math. (2)*, 34(3):461–479, 1933.
- [8] The LMFDB Collaboration. The L-functions and modular forms database. <https://www.lmfdb.org>, 2025. [Online; accessed January 2025].
- [9] J. H. Silverman. Lower bounds for height functions. *Duke Mathematical Journal*, 51(2):395–403, 1984.
- [10] J. H. Silverman. The difference between the weil height and the canonical height on elliptic curves. *Mathematics of computation*, 55(192):723–743, 1990.
- [11] G. Taylor. Nontorsion points of low height on elliptic curves over number fields. Available online at: https://maths.straylight.co.uk/low_height, last accessed on 10.06.2025.
- [12] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.6)*, 2025. <https://www.sagemath.org>.

CENTRE FOR MATHEMATICAL SCIENCES, UNIVERSITY OF CAMBRIDGE, CAMBRIDGE, UK
Email address: `sc2173@cam.ac.uk`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS AT AUSTIN, AUSTIN, TEXAS, USA
Email address: `john.m.clark@utexas.edu`

MATHEMATICAL INSTITUTE, LEIDEN UNIVERSITY, LEIDEN, THE NETHERLANDS
Email address: `c.k.l.dombrowsky@math.leidenuniv.nl`

MATHEMATICAL INSTITUTE, UTRECHT UNIVERSITY, UTRECHT, THE NETHERLANDS
Email address: `m.curcoiranzo@uu.nl`

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF VERMONT, BURLINGTON, VERMONT, USA
Email address: `Krystal.Maughan@uvm.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO AT BOULDER, BOULDER, COLORADO, USA
Email address: `eli.orvis@colorado.edu`