Experimental investigations on Lehmer's conjecture for elliptic curves

Sven Cats, John Michael Clark, Charlotte Dombrowsky, Mar Curcó 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 [**6**]. 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*

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

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 $N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ for the norm map and see Definition 2.1 for the height function $h : \mathbb{P}^1(\overline{K}) \to \mathbb{R}_{\geq 0}$. Consider the quantity $M_E = \max\{h(j_E), \log|N_{K/\mathbb{Q}}\Delta_E|, 1\}$.

Conjecture 1.2 (Lang). *Let*

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

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. Background on heights

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 $x : E(\overline{K}) \to \mathbb{P}^1(\overline{K})$ denote the map taking the x-coordinate and $h : \mathbb{P}^1(\overline{K}) \to \mathbb{R}_{\geq 0}$ the (absolute logarithmic) Weil height on $\mathbb{P}^1(\overline{K})$, as defined in [**5**], Section B.2. By a standard abuse of notation,

16 Jun 2025 09:18:47 PDT
250131-Orvis Version 2 - Submitted to LuCaNT

we also denote by $h : E(\overline{K}) \to \mathbb{R}_{\geq 0}$ the map defined by $P \mapsto h(x(P))$.
We denote the canonical height on E/K by

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

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

3. Computing minimal heights over field extensions

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

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

Consider the infimum

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

Remark 3.1. The first property ensures that whenever $F \in \mathscr{F}$ and $P \in E(F)$, the set $\mathscr{F}$ also contains the minimal field of definition $K(P)$ of P. The second property ensures that the subset of number fields in $\mathscr{F}$ of discriminant bounded by a given value is finite. In turn, using (for example) Lemma 3.2 below, this implies that a Northcott property holds for all fields in $\mathscr{F}$: There are finitely many points of bounded height on E over fields in $\mathscr{F}$. Thus the minimum height of such points exists and it follows that $C_{E,\mathscr{F}} > 0$. The fact that $C_{E,\mathscr{F}} > 0$ also follows directly from Theorem 3.3 and it is predicted by Conjecture 1.1 since $C_{E,\mathscr{F}} \geq C_E$.

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

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

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

$$\left|h(P) - \hat{h}(P)\right| \leq B_E \tag{1}$$

for all $P \in \cup_{F\in\mathscr{F}} E(F)$, see for example [**9**] 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 3.1.

Lemma 3.2. *Let $D \in \mathbb{R}_{\geq 0}$, $F \in \mathscr{F}$, 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*

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

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 $P \in E(F) - E(F)_{\mathrm{tors}}$ satisfying $K(P) = F$. Further, if $[F : K] = [F' : K]$, then $\Delta(D, E, F) = \Delta(D, E, F')$.

Proof. By Theorem 2 in [**8**] 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 $\Delta(D, E, F)$. □

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

Theorem 3.3. *Let $D' \in \mathbb{R}_{\geq 0}$ be such that $C_{E,\mathscr{F}} \leq D'$ and*

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

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

Proof. By our initial assumptions on $\mathscr{F}$, the set $\{[F : K] : F \in \mathscr{F}\}$ is finite. Therefore, we can define $\Delta = \max\{\Delta(D', E, F) : F \in \mathscr{F}\}$. The set $\mathscr{F}_\Delta = \{F \in \mathscr{F} : |\Delta_F| \leq \Delta\}$ is finite by the Hermite–Minkowski Theorem, and hence its subset $\mathscr{F}' \subset \mathscr{F}_\Delta$ is also finite. Lemma 3.2 implies that $C_{E,\mathscr{F}'} = C_{E,\mathscr{F}}$. □

In principle, we can therefore compute $C_{E,\mathscr{F}}$ as follows: Do an initial search to find $F' \in \mathscr{F}, P' \in E(F')$ with $K(P') = F'$ such that $D' = \hat{h}(P')[F' : K]$ is small. Then $C_{E,\mathscr{F}} \leq D'$ and we write $\mathscr{F}' \subset \mathscr{F}$ for the associated finite set of fields from Theorem 3.3. 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 $\mathscr{F}'$ to be considered later. For each $F \in \mathscr{F}'$ do a finite search to find the points $P \in E(F)$ such that

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

If $\mathscr{F}'$ is not too large[1] 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 $F_E \in \mathscr{F}$ and a $P_E \in E(F_E) - E(F_E)_{\text{tors}}$ such that $C_{E,\mathscr{F}} = \hat{h}(P_E) \cdot [F_E : K]$.

3.1. A modified CPS height bound. Cremona, Prickett and Siksek describe a bound for $h(P) - \hat{h}(P)$ where the point P lies in a fixed number field K in [**3**]. We refer to this as the CPS height bound. While this bound is sharper than the one proved by Silverman in [**9**], it depends on the number field K. We modify this result to compute an upper bound for all points P in quadratic extensions of $\mathbb{Q}$. Let K_ν be the completion of K at ν and let Δ_ν^{min} be the discriminant of the minimal model of E over K_ν. Then we have the following:

LEMMA 3.4. *Let $E/\mathbb{Q}$ be an elliptic curve. Let K be a quadratic extension. Let $M_1 := \max\{2\log(\epsilon_{\nu_{\mathbb{C}}}), 2\log(\epsilon_{\nu_{\mathbb{R}}})\}$, and $M_p := \max_{\nu|p}\{\frac{2}{[K_\nu:\mathbb{Q}_\nu]}(\alpha_\nu + \frac{1}{6}\text{ord}_\nu(\Delta_E/\Delta_\nu^{min}))\log(q_\nu)\}$. Then for all points $P \in E(K)$, we have:*

$$h(P) - \hat{h}(P) \leq \frac{M_1}{6} + \frac{1}{2}\sum_{p|\Delta_E} M_p.$$

The definitions of α_ν, ϵ_ν and q_ν can be found in [**3**]. *Moreover, there are only finitely many values of M_1 and M_p as K ranges over all quadratic extensions.*

PROOF. To keep the presentation succinct, we assume the reader is familiar with the bound in Theorem 1 of [**3**], and explain only how to modify this bound to apply over all quadratic fields simultaneously. The bound from Theorem 1 in [**3**] is given as a sum over archimedean and a sum over non-archimedean places. For the sum over archimedean places, we only need to take into account the complex valuation or twice the real valuation, depending on whether K is real or imaginary. This yields M_1. For the sum over non-archimedean values, we first note that for any valuation above a prime $p \nmid \Delta_E$, the term in the sum is zero. Thus it suffices to look at valuations above primes p dividing the discriminant of the elliptic curve.

Let ν be a valuation above an odd prime p. Then K_ν is either $\mathbb{Q}_\nu$ or one of its three quadratic extensions. Hence the contribution of any such place is bounded by the maximum of $(\alpha_\nu + \frac{1}{6}\text{ord}_\nu(\Delta_E/\Delta_\nu^{\text{min}}))\log(q_\nu)$ over all four possibilities. If $K_v \cong \mathbb{Q}_p$, then p splits, so we will have two valuations above p, which means that we need to multiply the corresponding term with 2. For the prime 2, the idea is the same, except that K_ν is isomorphic to either $\mathbb{Q}_2$ or one of its seven quadratic extensions. □

We note that Peter Bruin has given [**2**] a method to compute the supremum of $h(P) - \hat{h}(P)$ for an elliptic curve in Weierstrass form over all points in $\overline{\mathbb{Q}}$. We use the bound in Lemma 3.4 instead of this result both because of the possibility that Lemma 3.4 gives a smaller bound, since we consider only quadratic extensions, and because of its ease of implementation.

4. Computational Results

We implemented the ideas in Section 3 in the case of quadratic fields using MAGMA version 21.2-2[**1**]. In particular, for every elliptic curve in the Cremona database [**7**] of conductor at most 3,000, we conducted an initial search to find points of small height. We then computed a bound $\Delta = \Delta(D', E, F)$ as in Lemma 3.2, using the height bound in Lemma 3.4 as our B_E. For curves where the resulting bound Δ was less than 10^5, we searched for points of height at most 5 over all quadratic fields with $|\Delta_K| \leq \Delta$. The choice of searching for points of height at most 5 is arbitrary, but we almost always found such points, see Section 4.1. In this case, the point of smallest canonical height found over these quadratic fields is provably the point of smallest height on E over any quadratic field. In order to keep the computations feasible, for curves where the resulting bound was greater than 10^5, we searched only over quadratic fields with $|\Delta_K| \leq 1,000$. Here again, the choice of the upper-bound is arbitrary. We think the chosen bound is reasonable as in the provable cases the point of smallest height was usually found lying in a field with discriminant in this range, see Section 4.1. The resulting dataset is available, along with the code used to produce it at https://github.com/EliOrvis/LehmersConjectureForECs. The dataset contains 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;
- a flag indicating whether the point is provably the smallest over all quadratic fields.

REMARK 4.1. 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

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

points over quadratic fields. Implementing these changes could improve our algorithm. We thank an anonymous referee for this suggestion.

In this section we summarize the resulting data, and make some observations about its implications for Conjectures 1.1 and 1.2.

4.1. Description of data. We ran our code 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. Of these, we provably found the point of smallest height over all quadratic fields for 728 curves. For 542 curves, there were no non-torsion points of height smaller than five for any quadratic field we searched, 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

$$(27, -119, 1) \quad \text{on the elliptic curve} \quad y^2 + xy + y = x^3 + x^2 - 2990x + 71147, \tag{3}$$

which has Cremona label 1470l1, and height $0.0099641079999\ldots$.

We note that the point in (3) has height less than $1/100$, making it competitive with the points of small height on curves over $\mathbb{Q}$ found in Elkies table [**4**]. At the same time, Taylor found points of much smaller height on elliptic curves defined over quadratic fields [**10**] 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. These fields remained unchanged 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 137 curves, followed by $\mathbb{Q}$ with 117, and $\mathbb{Q}(\sqrt{-4})$ with 100. Finally, we note that among curves where we have provably found the point of smallest height over all quadratic fields, this point is always defined over a field K with $|\Delta_K| \leq 1,000$. Thus, we suspect that for many of the curves where our discriminant bound was larger than 10^5, the point in our dataset is in fact the smallest over all quadratic fields.

4.2. Remarks on Conjectures 1.1 and 1.2. We performed some preliminary investigations into Conjectures 1.1 and 1.2 using the data we collected. Over all elliptic curves in our dataset, the curve and point described in (3) represents the smallest lower bound obtained for Conjecture 1.1. To investigate Conjecture 1.2, we computed the quantity $L(E) := \frac{H_E}{\max\{1, h(j_E), \log(\Delta_E^2)\}}$ for all elliptic curves in our database, where H_E is the minimum height of a point found in a quadratic field. Figures 1 and 2 display $1/L(E)$ on the y-axis, and the conductor, and log of the discriminant, respectively on the x-axis.

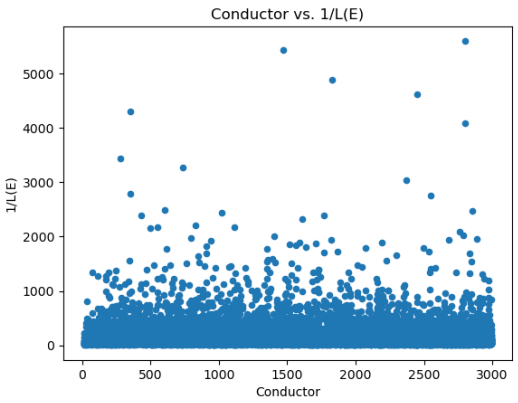

FIGURE 1. Conductor vs. constant in 1.2

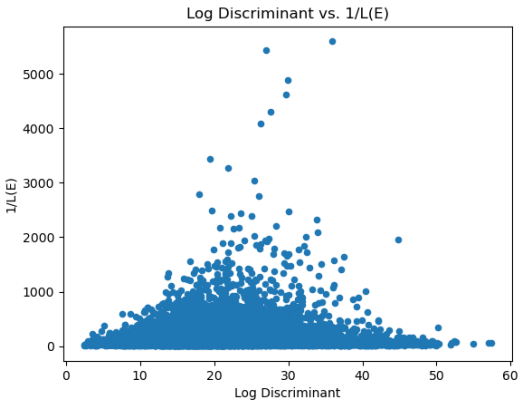

FIGURE 2. Log Discriminant vs. constant in 1.2

Because we are graphing $1/L(E)$, points that appear high on the y-axis correspond to particularly low values of $L(E)$. Although neither shows a clear correlation, there appears to be a tendency in our dataset for particularly low values of $L(E)$ to occur on curves with discriminant between roughly e^{20} and e^{35}. It is possible that this reflects a bias in the set of curves that we considered, however, since this range of discriminants contains a disproportionate number of the curves in our dataset.

5. Future work

There are several avenues available for extending this work. The first is to improve the completeness of our current dataset. One profitable extension would be to improve the efficiency of our search so that we can prove we have found the point of smallest height in more cases. This search is amenable to parallel processing since the computations over each quadratic extension are independent. In the future, we plan to implement this parallel algorithm to improve the completeness of our dataset.

The next avenue for exploration is to apply the same computational approach to fields of larger degree. We recall that the result of Lemma 3.2 holds for extensions of $\mathbb{Q}$ of any degree, and Lemma 3.4 can be suitably modified, or replaced with the bound of Bruin [**2**]. Working with extensions of degree larger than 2 introduces the challenge of enumerating all extensions of $\mathbb{Q}$ of bounded discriminant, however. At least in the case of cubic fields, this could be overcome by leveraging the database already compiled in the LMFDB. Finally, we note that the two quadratic fields most likely to contain points of small height were the two cyclotomic quadratic fields. We plan to investigate this phenomenon further by searching for points of small height over cyclotomic fields of larger degree.

Lastly, theoretical improvements on Theorem 2 of [**8**] or Lemma 3.4 would significantly reduce the number of searchable quadratic fields, which would improve our algorithm, and hence enlarge the database.

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 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] 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.

[5] M. Hindry and J. H. Silverman. Diophantine Geometry. Springer-Verlag, New York, 2000. An Introduction.

[6] D. H. Lehmer. Factorization of certain cyclotomic functions. Ann. of Math. (2), 34(3):461–479, 1933.

[7] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2025. [Online; accessed January 2025].

[8] J. H. Silverman. Lower bounds for height functions. Duke Mathematical Journal, 51(2):395–403, 1984.

[9] J. H. Silverman. The difference between the weil height and the canonical height on elliptic curves. Mathematics of computation, 55(192):723–743, 1990.

[10] 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.

University of Cambridge
Email address: `sc2173@cam.ac.uk`

University of Texas at Austin
Email address: `john.m.clark@utexas.edu`

Leiden University
Email address: `c.k.l.dombrowsky@math.leidenuniv.nl`

Utrecht University
Email address: `m.curcoiranzo@uu.nl`

University of Vermont
Email address: `Krystal.Maughan@uvm.edu`

Department of Mathematics, University of Colorado at Boulder
Email address: `eli.orvis@colorado.edu`