Some experiments on Lehmer's Conjecture for Elliptic Curves

Sven Cats, John Michael Clark, Mar Curcó Iranzo, Charlotte Dombrowsky, Krystal Maughan, **Eli Orvis**

July 8, 2025

Introduction

Let E/K be an elliptic curve over a number field K, h denote the logarithmic height, and $\hat{h}$ denote the canonical height.

Introduction

Let E/K be an elliptic curve over a number field K, h denote the logarithmic height, and $\hat{h}$ denote the canonical height. We have the following conjectures about $\hat{h}(P)$ for $P \in E$, first varying K, then varying E:

Introduction

Let E/K be an elliptic curve over a number field K, h denote the logarithmic height, and $\hat{h}$ denote the canonical height. We have the following conjectures about $\hat{h}(P)$ for $P \in E$, first varying K, then varying E:

Conjecture (Lehmer's Conjecture)

Fix E/K. Let

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

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

Introduction

To state Lang's conjecture, let
$M_E = \max\{h(j_E), \log|N_{K/\mathbb{Q}}\Delta_E|, 1\}$.

Introduction

To state Lang's conjecture, let
$M_E = \max\{h(j_E), \log|N_{K/\mathbb{Q}}\Delta_E|, 1\}$.

Conjecture (Lang's Conjecture)

Fix K, and $d \in \mathbb{Z}_{\geq 1}$. Define

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

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

Introduction

1. While experimental work on Lehmer's Conjecture for polynomials is extensive, the work on the case of elliptic curves is more limited.

Introduction

1. While experimental work on Lehmer's Conjecture for polynomials is extensive, the work on the case of elliptic curves is more limited.
2. Previous work by Elkies, Taylor, and others focused on targeted searches in families of curves likely to contain points of low height.

Introduction

1. While experimental work on Lehmer's Conjecture for polynomials is extensive, the work on the case of elliptic curves is more limited.
2. Previous work by Elkies, Taylor, and others focused on targeted searches in families of curves likely to contain points of low height.
3. Our goal was to preform a broad search: we use the Cremona Database to search by conductor, and focus on the case of quadratic extensions of $\mathbb{Q}$.

Introduction

1. While experimental work on Lehmer's Conjecture for polynomials is extensive, the work on the case of elliptic curves is more limited.
2. Previous work by Elkies, Taylor, and others focused on targeted searches in families of curves likely to contain points of low height.
3. Our goal was to preform a broad search: we use the Cremona Database to search by conductor, and focus on the case of quadratic extensions of $\mathbb{Q}$.
4. Using a modified version of the Cremona-Prickett-Siksek bound, we can verify that we have found the point of smallest height over any quadratic field in some cases.

Ingredients for search algorithm

The primary ingredients for our search algorithm are:

Ingredients for search algorithm

The primary ingredients for our search algorithm are:

1. An initial search for points P with small $h(P)$.

Ingredients for search algorithm

The primary ingredients for our search algorithm are:

1. An initial search for points P with small $h(P)$.
2. A bound B_1 depending on E, $r \in \mathbb{R}_{>0}$, and $[F : K]$, such that

$$|\Delta_F| \geq B_1 \implies \hat{h}(P) \geq \frac{r}{[F : K]}, \text{ for } P \in E(F) \setminus E(F)_{\text{tors}}.$$

Ingredients for search algorithm

The primary ingredients for our search algorithm are:

1. An initial search for points P with small $h(P)$.
2. A bound B_1 depending on E, $r \in \mathbb{R}_{>0}$, and $[F:K]$, such that
$$|\Delta_F| \geq B_1 \implies \hat{h}(P) \geq \frac{r}{[F:K]}, \text{ for } P \in E(F) \setminus E(F)_{\text{tors}}.$$
3. A bound B_2 depending on E, $[F:K]$ such that
$$h(P) - \hat{h}(P) \leq B_2, \text{ for } P \in E(F) \setminus E(F)_{\text{tors}}.$$

Algorithm in the quadratic case

Putting these together, our strategy for each curve E is:

Algorithm in the quadratic case

Putting these together, our strategy for each curve E is:

1. Preform the initial search to find a point with $r := \hat{h}(P)$ small.

Algorithm in the quadratic case

Putting these together, our strategy for each curve E is:

1. Preform the initial search to find a point with $r := \hat{h}(P)$ small.
2. Use $2r, E$ as input to the bound B_1, giving a limit on the discriminants that we need to search.

Algorithm in the quadratic case

Putting these together, our strategy for each curve E is:

1. Preform the initial search to find a point with $r := \hat{h}(P)$ small.
2. Use $2r, E$ as input to the bound B_1, giving a limit on the discriminants that we need to search.
3. Compute the bound B_2 for E over quadratic fields, giving a bound on the logarithmic height of points that need to be searched on each quadratic field.

Algorithm in the quadratic case

Putting these together, our strategy for each curve E is:

1. Preform the initial search to find a point with $r := \hat{h}(P)$ small.
2. Use $2r, E$ as input to the bound B_1, giving a limit on the discriminants that we need to search.
3. Compute the bound B_2 for E over quadratic fields, giving a bound on the logarithmic height of points that need to be searched on each quadratic field.
4. Preform the search over the finitely many discriminants up to the specified logarithmic height bound.

Algorithm: failure cases

The algorithm can fail in two ways:

Algorithm: failure cases

The algorithm can fail in two ways:

1. No points are found during the initial search.

Algorithm: failure cases

The algorithm can fail in two ways:

1. No points are found during the initial search.
2. The bound on discriminants is too large to be feasible.

Algorithm: failure cases

The algorithm can fail in two ways:

1. No points are found during the initial search.
2. The bound on discriminants is too large to be feasible.

Both are arbitrary cutoffs, and we handled them by:

Algorithm: failure cases

The algorithm can fail in two ways:

1. No points are found during the initial search.
2. The bound on discriminants is too large to be feasible.

Both are arbitrary cutoffs, and we handled them by:

1. Excluding in the first case,

Algorithm: failure cases

The algorithm can fail in two ways:

1. No points are found during the initial search.
2. The bound on discriminants is too large to be feasible.

Both are arbitrary cutoffs, and we handled them by:

1. Excluding in the first case,
2. Performing a search for points of small height on quadratic fields up to discriminant $1,000$ in the second.

Dataset details

Our dataset contains the following fields:

- the Cremona label for the curve;
- the discriminant of the quadratic field over which the point of smallest height that we found is defined;
- the coordinates of the point of smallest height;
- the height of this point;
- a flag indicating whether the point is provably the smallest over all quadratic fields.

Overview of computation and data

1. We implemented the previous search algorithm in Magma and searched curves with conductor at most $3,000$.

Overview of computation and data

1. We implemented the previous search algorithm in Magma and searched curves with conductor at most $3,000$.
2. In a little over 800 hours of computation, we provably found the point of smallest height over any quadratic field for 728 elliptic curves.

Overview of computation and data

1. We implemented the previous search algorithm in Magma and searched curves with conductor at most $3,000$.
2. In a little over 800 hours of computation, we provably found the point of smallest height over any quadratic field for 728 elliptic curves.
3. We re-encountered points found by Elkies, as well as finding other points with similarly small height.

Preliminary investigations

We performed some preliminary data exploration, investigating the constant in Lang's conjecture over conductor and discriminant ranges:

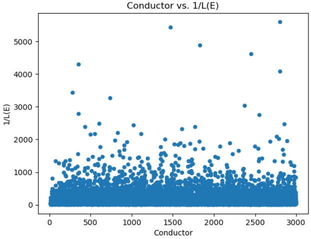

Figure: Conductor vs. constant in Lang's Conjecture

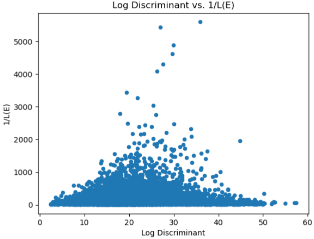

Figure: Log Discriminant vs. constant in Lang's Conjecture

Thank you!