Canonical Height on Elliptic Curves

Adrian Neff, Prof. Ghaith Hiary

Introduction

An elliptic curve over the rational numbers is of the form:

$$y^2 = x^3 + ax + b; \quad a, b \in \mathbb{Q}$$

Let E be the set of rational points on the curve. The set E can be endowed with an *additive group structure*.

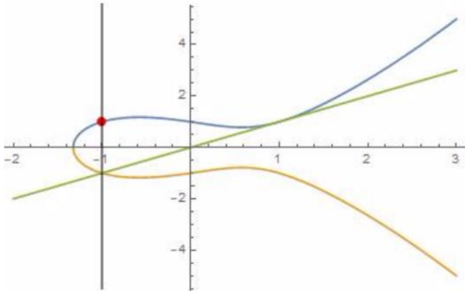


Figure 1: A geometric example of the operation called point addition on elliptic curves.

Various size measures called height functions are defined on E, such as the logarithmic height (1) and the canonical height (2):

$$h(z) = \log(\max\{|x|, |y|\}); \quad z = \frac{x}{y} \in \mathbb{Q} \qquad (1)$$

$$\hat{h}(P) = \lim_{n \to \infty} \frac{h_x(nP)}{n^2} \qquad (2)$$

In 1978, number-theorist Serge Lang conjectured a lower bound for the canonical height. This project is concerned with the form of the conjecture which states that there exist constants C_1 and C_2 such that:

$$\hat{h}(P) \geq C_1 \log(|\Delta_{min}|) - C_2; \quad C_1, C_2 > 0$$

$$\Delta = -16(4a^3 + 27b^2)$$

The aim is to computationally test this conjecture for a family of elliptic curves with a common rational point (i.e. a common rational solution) P = (1,1). As a result, we produce a new conjecture on the height of this common point.

$$y^2 = x^3 + ax - a; \quad P = (1,1)$$

Methods

All computations were performed in either Mathematica or Sage. The canonical height of the common point in the family of elliptic curves under consideration was calculated using both a built-in function in Sage and an approximation procedure that we implemented in Mathematica based on a method of doubling a point in E.

Results

- The height of the point P = (1,1) grew according to the lower bound in the Lang conjecture.
- A trend in the data arose indicating the height of the point was dependent on the value of the coefficient a modulo 4 of the curve in the family.
- As a result, we conjectured an explicit formula for the height of the common point in the family of curves:

$$\hat{h}(P) = \begin{cases} \frac{1}{2}\log(a), & \text{if } a \equiv 0, 2 \bmod 4 \\ \frac{1}{2}\log(a) - \frac{1}{2}\log(2), & \text{if } a \equiv 1 \bmod 4 \\ \frac{1}{2}\log(a) - \frac{2}{3}\log(2), & \text{if } a \equiv 3 \bmod 4 \end{cases}$$

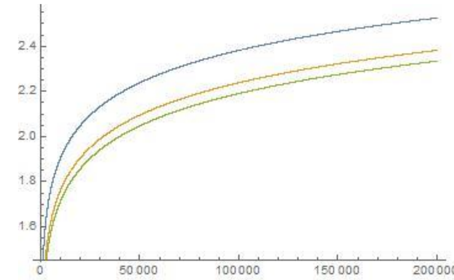
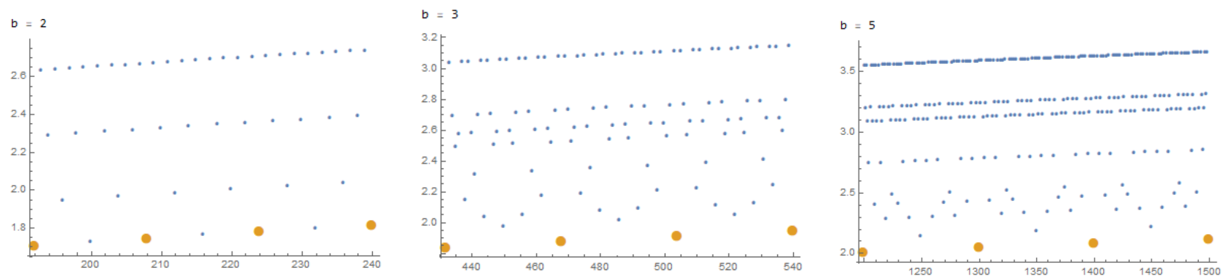


Figure 2: The height of the point (1,1) for the first 200,000 curves in the family.

- When looking at other families of curves (shown below), a similar trend arose relating the height of the common point to the prime factorization of the coefficient b.
- The trend in the other families suggests the possibility of similar conjectural formulas.

$$y^2 = x^3 + ax + b^2; \quad P = (0, b)$$



Figure(s) 3: Examples of the trends in the heights found in other families of curves with a different varying coefficient.

Conclusion

- The data gathered supports the validity of the Lang conjecture. In addition, we obtained a conjectural formula (shown above) for the height of the common point P = (1,1) on the original family.
- A possible future direction is to conjecture similar formulas for other natural families of elliptic curves.

References

Lang, Serge. (1978). *Elliptic Curves: Diophantine Analysis*
Silverman, Joseph. (2009). *The Arithmetic of Elliptic Curves*
Silverman, Joseph. (1992). *Rational Points on Elliptic Curves*

THE OHIO STATE UNIVERSITY