Rational Points of Low Height on Elliptic Curves

Ellen E. Eischen*

January 19, 2002

Mathematics Department
Princeton University
Princeton, NJ 08544

Abstract

Consider a one-parameter family of elliptic curves, $y^2 = x^3 + A(t)x + B(t)$, where $A(t)$ and $B(t)$ are polynomials with integer coefficients. "Height" is a measurement of the "arithmetic complexity" of a rational point on the curve. Height has several significant uses. For example, it is used in proving that the Mordell-Weil group is finitely generated. How does the height of the lowest point vary among the curves in each family? If a curve has higher than predicted rank, then does it also have a point of "low" height?

*E-mail: `eeischen@math.princeton.edu`

1 Introduction

Consider elliptic curves, $y^2 = x^3 + Ax + B$, in which A and B are integers, and consider the set of rational solutions (x, y) to this equation. This set of points forms an abelian group, and we denote it as $E(\mathbb{Q})$.

In order to proceed, we will need a way to distinguish between points of varying "arithmetic complexity." For this reason, we will shortly introduce a notion of height. Height is used in proving the Mordell-Weil Theorem and in computing the the Mordell-Weil group.

2 Naive Height

Consider the numbers 1 and $\frac{999999999}{1000000000}$. Although they differ by only $\frac{1}{1000000000}$, the second number is more "complex" than the first one. *Naive height* provides a way to measure the "arithmetic complexity" of a point.

Definition 2.1 *The* **naive height***, h_0, of a point $P = (x, y)$ on an elliptic curve is defined to be*

$$h_0(P) = \log \max(|p|, |q|), \tag{2.1}$$

where $x = \frac{p}{q}$ in lowest terms.

An interesting property about naive height is that given a number $N \geq 0$, only finitely many points in $E(\mathbb{Q})$ have naive height less than or equal to N. To see this, note that there are only finitely many integers, n, such that $\log n \leq N$. Therefore, there are only finitely many numbers $x = \frac{p}{q}$, such that both $\log p$ and $\log q$ are less than N. For each $x-$coordinate, there are at most two distinct corresponding $y-$values. Hence, the number of points with height $\leq N$ is bounded.

Let T be a positive integer. We have the following asymptotic relation between the number of points with naive height $\leq T$ and the geometric rank of a curve as $T \to \infty$.

Lemma 2.2 *Let E be an elliptic curve with geometric rank r. Then, as $T \to \infty$,*

$$\left\{P \in E(\mathbb{Q}) : h_0(P) \leq T\right\} \begin{cases} = \# Tor E(\mathbb{Q}) & if \quad r = 0 \\ \sim \frac{\# Tor E(\mathbb{Q}) \Omega_r}{R^{1/2}_{E/\mathbb{Q}}} T^{r/2} & if \quad r > 0 \end{cases} \tag{2.2}$$

where Ω_r is the unit ball in $\mathbb{R}^r$, and $R_{E/\mathbb{Q}} = \det(\langle P_i, P_j \rangle)$ with the $\{P_i\}$ a basis for the free group.

The proof, which uses Euclidean analysis, is given in [Kn 106].

As demonstrated by Lemma 2.2, naive height is useful because of its relationship to geometric rank. Also, using naive height, we are able to prove that the Mordell-Weil group is finitely generated.

Because the rank is determined only by the points of infinite order and not by the torsion points, it will be useful to have a measure of height that differentiates between torsion and non-torsion points. We will see in the next section that *canonical height* provides a way to distinguish torsion points from points of infinite order.

3 Canonical Height

Although naive height is useful because of its relationship to the rank, it tells us nothing about the order of the point. When considering rank, it is useful to know which points actually contribute to the rank. For this reason, we introduce canonical height.

Definition 3.1 *The* **canonical height**, *h, of a point $P = (x, y)$ is*

$$h(P) = \lim_{n\to\infty} \frac{h_0(2^n P)}{4^n}. \tag{3.1}$$

From now on, h_o will denote naive height, and h will denote canonical height. The usefulness of canonical height is made clear by the fact that $h(P) = 0$ if and only if P is in the torsion group and that $h(P)$ converges for each point P, as will be shown in the proofs of Lemmas 3.7 and 3.6

We first must prove several preliminary lemmas, however.

N.B: We will use $x(P)$ to denote the x coordinate of a point P.

The *Duplication Formula,* which is presented below, is a formula for $x(2P)$. This is a standard result, and the interested reader is refered to [ST 31].

DUPLICATION FORMULA: We have the following formula for the $x(2P)$, where P is a point on the elliptic curve of the form $y^2 = x^3 + Ax + B$:

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B} \tag{3.2}$$

In showing that $h(P)$ converges, we will need the following lemma:

Lemma 3.2 *[Kn 95]Let $P = (x, y)$. The naive height, $h_o(P)$, satisfies*

$$h_0(2P) = 4h_0(P) + O(1), \tag{3.3}$$

where $O(1)$ is bounded and does not depend on P.

Proof: Let $P' = 2P = (x', y') \neq \infty$. Then, from Formula 3.2, we have

$$x' = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}. \tag{3.4}$$

Now let $x = p/q$, where p and q are relatively prime integers. Replacing x with p/q in the above equation yields that $x' = p'/q'$, where

$$p' = p^4 - 2Ap^2q^2 - 8Bpq^3 + A^2q^4 \tag{3.5}$$

and

$$q' = 4qp^3 + 4Apq^3 + 4Bq^4. \tag{3.6}$$

First we will prove that

$$h_0(2P) \leq 4h_0(P) + \kappa, \tag{3.7}$$

where κ is a constant dependent only on the curve.

Let $m = (p', q')$. Let $p'' = \frac{p'}{m}$ and $q'' = \frac{q'}{m}$ so that $x' = \frac{p''}{q''}$ in lowest terms. Hence,

$$\begin{aligned}
\max(|p''|, |q''|) &\leq \max(|p'|, |q'|) \\
&\leq \max(|p|, |q|)^4 \times \max(1 + 2|A| + 8|B| + A^2, 4(1 + |A| + |B|)) \\
&= C \max(|p|, |q|)^4, \qquad (3.8)
\end{aligned}$$

where $C = \max(1 + 2|A| + 8|B| + A^2, 4(1 + |A| + |B|))$. (N.B: The first inequality follows from the fact that $p'' = p'/m$ and $q'' = q'/m$. The second inequality follows from the equations for p' and q'.)

Therefore,

$$h_o(2P) = \log \max(|p''|, |q''|) \leq logC + 4 \log \max(|p|, |q|) = \log C + 4h_0(P), \tag{3.9}$$

which yields

$$h_o(2P) \leq 4h_0(P) + C', \tag{3.10}$$

where $C' = \log C$.

Now, we will prove the opposite inequality:

$$h_o(2P) \geq 4h_0(P) + \kappa',$$

where κ' is a constant dependent only on the curve.

Let $\Delta \neq 0$ be the discrimant of $x^3 + Ax + B$. We state without proof the following two identities:

$$4\Delta q^7 = (3p^3 - 5Apq^2 - 27Bq^3)q' - 4(3p^2q + 4Aq^3)p' \tag{3.11}$$

$$\begin{aligned} 4\Delta p^7 &= -(A^2Bp^3 + (5A^4 + 32AB^2)p^2q^2 + (26A^3B + 129B^3)pq^2 \\ &\quad -3(A^5 + 8A^2B^2)q' - 4((4A^3 + 27B^2)p^3 - A^2Bp^2q \\ &\quad +(3A^4 + 22AB^2)pq^2 + 3(A^3B + 8B^3)q^3)p'. \end{aligned} \tag{3.12}$$

The interested reader is refered to [Kn96].

These equations yield

$$\max(|p|,|q|)^7 \leq C'' \max(|p|,|q|)^3 \max(|p'|,|q|), \tag{3.13}$$

where C'' is a constant dependent only on the curve.

Therefore,

$$\max(|p|,|q|)^4 \leq C'' \max(|p'|,|q'|). \tag{3.14}$$

From the above equation for $4\Delta p^7$, observe that $m|4\Delta q^7$ and $m|4\Delta p^7$. Since gcd(p,q)=1, it follows that $m|4\Delta$. Therefore, m is bounded by 4Δ.

Hence, we obtain the following inequality:

$$max(|p|,|q|) \leq C^* max(|p''|,|q''|). \tag{3.15}$$

Combining the previous two inequalities yields:

$$max(|p|,|q|)^4 \leq C''C^* max(|p''|,|q''|). \tag{3.16}$$

Thus, we have:

$$\begin{aligned} 4h_o(P) &= 4\log\max(|p|,|q|) \leq C^{**} + \log\max(|p''|,|q''|) \\ &= h_o(2P) + C^{**}, \end{aligned} \tag{3.17}$$

where $C^{**} = log(C''C^*)$, which proves the second main inequality. Inequalities 3.10 and 3.17 together prove the lemma. ■

Although we have a definition for canonical height, we have not yet seen that canonical height converges for each point $P \in E(\mathbb{Q})$. The proofs of the following two lemmas show that $h(P)$ converges for each $P \in E(\mathbb{Q})$.

Lemma 3.3 (Kn) $\{\frac{h_o(2^nP)}{4^n}\}$ *is Cauchy.*

Proof: Recall that $h_o(2P) = 4h_o(P) + O(1)$. Hence, there exists a constant κ independent of P such that

$$|h_o(2P) - 4h_o(P)| \le \kappa.$$

Let N and M be integers such that $N \ge M \ge 0$. Then,

$$\begin{aligned}
|4^{-N}h_0(2^NP) - 4^{-M}h_0(2^MP)| &= |\sum_{n=M}^{N-1}(4^{-n-1}h_0(2^{n+1}P) - 4^{-n}h_0(2^nP))| \\
&\le \sum_{n=M}^{N-1} 4^{-n-1}|h_o(2^{n+1}P) - 4h_o(2^nP))| \\
&\le \sum_{n=M}^{N-1} 4^{-n-1}\kappa \\
&\le \frac{4^{-M}\kappa}{3}. \qquad (3.18)
\end{aligned}$$

Observe that as M and N go to ∞, the right hand side tends to zero, which proves the lemma. ■

Thus, we have that canonical height converges for each point P. We will now see that, in fact, the amount by which the canonical height differs from the naive height is bounded.

Lemma 3.4 $h(P) - h_o(P)$ *is bounded.*

Proof: From the above inequality, we have:

$$|4^{-N}h_0(2^NP) - 4^{-M}h_0(2^MP)| \le \frac{4^{-M}\kappa}{3}. \qquad (3.19)$$

Letting $M = 0$ and $N \to \infty$ yields

$$|h(P) - h_o(P)| \le \frac{\kappa}{3}, \qquad (3.20)$$

which proves the lemma. ■

Lemma 3.5 $h(2P) = 4h(P)$.

Proof: This follows directly from the fact the definition of $h(P)$ and the fact that $h_o(2P) = 4h(P) + \kappa$, where κ is a constant independent of P. ∎

Note it was not as simple to compute the naive height of $2P$. From Lemma 3.5, however, we obtain a simple formula for computing the canonical height of $2P$.

Now, we are able to prove Lemmas 3.7 and 3.6, which demonstrate the usefulness of canonical height in distinguishing points of infinite order from torsion points.

Lemma 3.6 *If $P \in E(\mathbb{Q})$ is a torsion point, then $h(P) = 0$.*

Proof: If P is a torsion point, then $2^n P$ takes on only finitely many values. Therefore, $h_0(2^n P)$ is bounded from above by a positive integer M. Therefore, we have $h(P) \leq \lim_{n\to\infty} \frac{M}{4^n} = 0$. ∎

Lemma 3.7 *If $P \in E(\mathbb{Q})$ has infinite order, then $h(P) > 0$.*

Proof: (by contradiction) Let $P \in E(\mathbb{Q})$ have infinite order, and suppose $h(P) = 0$. Then, by Lemma 3.5, $h(2P) = 4h(P)$. Therefore, $h(2^n P) = 4^n h(P) = 4^n * 0 = 0$, for all non-negative integers n. By Lemma 3.2, then there exists a constant N such that $N \geq |h_o(2^n P) - h(2^n P)| = |h_o - 0| = h_0$ for every non-negative integer n. Hence, we have that infinitely many points $P \in E(\mathbb{Q})$ have height less than or equal to N, which clearly contradicts the fact that $E(\mathbb{Q})$ can only has only finitely many points with height less than or equal to N. Therefore, we must have $h(P) \neq 0$. From the equation for canonical height, we see that canonical height is bounded below by zero. Therefore, we have $h(P) > 0$, which proves the lemma. ∎

We now see that canonical height, unlike naive height, differentiates between torsion and non-torsion points.

4 Computational Techniques

Salman Butt and I wrote a program that finds rational points on elliptic curves. The user specifies a family of curves, upper and lower bounds for the parameter to the family, and a maximum naive height N. For each curve within the family, the program returns points with naive height $\leq N$. It returns the canonical height of each point along with the point.

For example, if the user inputs $N = 10000$, lets the bounds for the parameter be 2 and 100, and chooses the family $y^2 = x^3 - t^2 x + t^4$, then the output would output points of naive height $\leq N$ on each of the curves $y^2 = x^3 - 4x + 16$, $y^2 = x^3 - 9x + 81$, ..., $y^2 = x^3 - 10000x + 10^8$.

We developed three main methods to find points on the curve. We decided to use the last of the three methods described below:

4.1 First Method

The first method is motivated by the following lemma:

Lemma 4.1 *If $P = (x, y)$ is a rational point on an elliptic curve, then there exist integers a, b, and $c > 0$ with $gcd(a, c) = gcd(b, c) = 1$ such that when we write x and y in lowest terms,*

$$x = \frac{a}{c^2} \textit{ and } y = \frac{b}{c^3}. \tag{4.1}$$

Proof: Let a, b, α, and β be the integers such that

$$x = \frac{a}{\alpha} \text{ and } y = \frac{b}{\beta}, \tag{4.2}$$

when x and y are written in lowest terms with positive denominators. Then, we have that $\alpha \geq 0$ and $\beta \geq 0$. Substituting into the equation $y^2 = x^3 + Ax + B$ yields

$$\frac{b^2}{\beta^2} = \frac{a^3}{\alpha^3} + A\frac{a}{\alpha} + B. \tag{4.3}$$

Multiplying by $\alpha^3\beta^2$ yields

$$\alpha^3 b^2 = \beta^2 a^3 + A\beta^2\alpha^2 a + B\beta^2\alpha^3. \tag{4.4}$$

We will show that α^3 must equal β^2 by showing that both $\alpha^3|\beta^2$ and $\beta^2|\alpha^2$. Note that since β^2 is a factor of each of the terms on the right hand side of the above equation, β^2 must divide the left hand side of the equation. Since y is expressed in lowest terms, β does not divide b. Therefore, β^2 must divide α^3.

Notice that from the above equation, we must have that $\alpha|\beta^2 a^3$. Since x is expressed in lowest terms, α does not divide a. Therefore, it follows that $\alpha|\beta^2$. Therefore, each of the last three terms on the left hand side is divisible by α^2. Since the right hand side of the equation is also divisible by α^2, we have that $\alpha^2|\beta^2 a^3$, and therefore, since $\gcd(a, \alpha) = 1$, $\alpha^2|\beta^2$. Hence, $\alpha|\beta$. Now, we have that α^3 divides every term on the left hand side of the equation, except possibly the first term. Since α^3 divides the left hand side of the equation, it follows that α^3 does in fact divide the first term of the right hand side. That is, $\alpha^3|\beta^2$.

Therefore, since $\alpha^3|\beta^2$ and $\beta^2|\alpha^3$, we see that $\alpha^3 = \beta^2$. We now let $c = \frac{\beta}{\alpha}$. Note that c is an integer, since we proved above that $\alpha|\beta$. We now have

$$c^2 = \frac{\beta^2}{\alpha^2} = \frac{\alpha^3}{\alpha^2} = \alpha \tag{4.5}$$

and

$$c^3 = \frac{\beta^3}{\alpha^3} = \frac{\beta^3}{\beta^2} = \beta. \tag{4.6}$$

Hence $x = \frac{a}{c^2}$ and $y = \frac{b}{c^3}$.

■

In this method, the program searches through all integers a and c with naive height less than the user-specified value, where $\gcd(a, c) = 1$ and $c > 0$. I defined a type called *rational* and several opperations to make computation with rational numbers feasible. For example, $RATadd(x_1, x_2)$ returns the sum of the rational numbers x_1 and x_2 in lowest terms. Then, the program checks to see whether both the numerator and the denominator of $\frac{a}{c}^3 + A\frac{a}{c} + B$ are squares. If so, $\frac{a}{c^2}$ is the x-value of a point on the curve, and otherwise, it is not the x-value of a point on the curve.

4.2 Second Method

In this method, we look at the number

$$d = c^3\sqrt{(x_1^3 + Ax_1 + B)}, \tag{4.7}$$

where $x_1 = \frac{a}{c^2}$. If d is not an integer, we have that x_1 is not the x value of any points on the curve. If d is an integer, we use pari to determine whether or not $(x_1, \frac{d}{c^3})$ is on the curve.

4.3 Third Method

The third method is the method that we currently use and that we plan to use for future computations of height. We encountered several problems while writing the previous each of the versions, and this method addresses all the problems successfully.

When a previous version did not output all the points we expected, we learned that the *mod* function in the C programming language is not defined for negative numbers. To solve this problem, Salman wrote a new *mod* function that is defined for negative numbers.

Also, in order to handle large numbers, we do as many of our computations as possible mod the first ten primes. For example, before checking to see whether a large number is prime, we first check that it is a prime.

If $d = c^6[x^3 + Ax + B]$ is a square mod the first ten primes, then we check whether $\sqrt{d}$ and $[\sqrt{d}]$ differ by less than 10^{-3}, where $[u]$ denotes the greatest integer less than or equal to u.

If the difference between $\sqrt{d}$ and $[\sqrt{d}]$ is $\leq 10^{-3}$, then the candidate point is sent to the *Pari* function *ellisoncurve* to determine whether the point is on the curve. If it is on the curve, the curve outputs the point and its canonical height.

4.4 Computation of Height

It is clear that it would be computationally difficult to compute canonical height based on the definition given earlier:

$$h(P) = \lim_{n \to \infty} \frac{h_0(2^n P)}{4^n}. \tag{4.8}$$

There is, however, a more computationally feasible way to compute canonical height. This is known as the *global height* of a point P. The global height of P is computed as a sum of *local heights* of P.

Definition 4.2 *The global height, $\hat{h}(P)$, is a sum over all primes p of the local heights $\hat{h}_p(P)$:*

$$\hat{h}(P) \;=\; \sum_{p \leq \infty} \hat{h}_p(P) \tag{4.9}$$

The interested reader is referred to [Cr 56] for the precise formula for local height. The important characteristic of local height is that for all but finitely many primes p, $\hat{h}_p(P) = 0$. Therefore, most of the terms in the sum for $\hat{h}(P)$ are 0. Also, for each prime p, $\hat{h}_p(P)$ is a rational multiple of $\log p$.

Therefore, global height provides a computationally feasible way of computing canonical height. For more information, the interested reader is referred to [Si].

5 What Comes Next

We have written a program that finds all the points with height less than or equal to a user-specified value for each curve in a family. Now that this program works, the next step is to study more curves. In particular, we would like to study height in the context of other properties of a curve. Also, we will now give our output to other people who need it to run their programs. For example, Adam Durrett's program uses the height-pairing matrix to compute the rank of curves. He needs a list of points on the curve to compute the rank of the curve. Once we know the rank of the curve, we can check to see whether curves with excess rank (higher rank than we have forced on the curve) have a point of "low" height. By "low" height, we mean a point with lower height than the points that were forced on the curve. (Therefore, the precise values that will be considered 'low" depend on the family.) Also, we would like to look at the distribution of points with low height in a given family to see if (and how) this relates to the conductor of the curve.

Now that we have written a program to locate rational points on the curve, we will be able to study computationally the relationship between height and other properties of the curve, as will future students who use our program.

6 Bibliography

[Cr] Cremonoa. *Algorithms for Modular Elliptic Curves,* Cambridge University Press, Cambridge, 1992.
[Kn] Knapp, Anthony W. *Elliptic Curves,* Princeton University Press, Princeton, 1992.
[Si] Silverman, Joseph. "Computing Heights on Elliptic Curves." *Mathematics of Computation,* Volume 51, Issue 183 (Jul., 1988), 339-358.
[ST] Silverman and Tate. *Rational Points on Elliptic Curves,* Springer-Verlag, New York, 1992.