# Heights

J.Roshardt, M.Schlatter

October 13, 2023

## 1 Introduction to heights

In the following, we will introduce the notion of heights and how it behaves under certain operations (e.g. adding two points on the curve). Furthermore, the height translates geometry on the curve into number theory. The height will be essential to prove Mordell's theorem. Our main reference is Chapter 3 of Silverman and Tate [1].

From now on, we consider a non-singular cubic curve in the weierstrass normal form $y^2 = f(x) = x^3 + ax^2 + bx + c$ with integer coefficients $a, b, c \in \mathbb{Z}$.

**Definition 1.1** (Height)**.** *The height of a rational number $x = \frac{m}{n} \in \mathbb{Q} \setminus \{0\}, \gcd(m,n) = 1$ is defined as*

$$H(x) = H(\frac{m}{n}) := max\{|m|, |n|\} \in \mathbb{Z}^{\geq 1}.$$

*(by convention $H(0) = 1$)*

**Example 1.1.** *$H(\frac{1}{2}) = 2 = H(\frac{3}{6})$ or $H(-\frac{9999}{20000}) = 20000$*

The height is a useful tool to measure the "complexity" of a rational point. Even though $\frac{1}{2}$ and $\frac{9999}{20000}$ have a similar absolute value, intuitively one would say that $\frac{9999}{20000}$ is more complicated than $\frac{1}{2}$ (in a number theoretic sense).

**Definition 1.2** (Height of a point)**.** *For a point $P = (x, y) \in C(\mathbb{Q})$ we define the height of $P$ to be the height of the $x-$coordinate:*

$$H(P) := H(x)$$

*and in the special case of $P = \mathscr{O}$ we define $H(\mathscr{O}) := 1$.*

**Definition 1.3** (Small height)**.** *The small height is defined as $h(P) := log(H(P)) \in \mathbb{R}^{\geq 0}$.*

We will want to compare $H(P + Q)$ to $H(P)H(Q)$. Since the logarithm transforms multiplication into addition it is reasonable to define the small height.

The goal is to prove that the group of rational points $C(\mathbb{Q})$ is finitely generated. To this end, we prove three lemmata.

## 2 Lemma 1: Finiteness Property

**Lemma 2.1.** *For any real number $M$, the set*

$$\{P \in C(\mathbb{Q}) : h(P) \leq M\}$$

*is finite.*

This lemma is quite straight forward once we proved result 2.1:

**Result 2.1** (Finiteness Property of the Height)**.** *The set of all rational numbers whose height is less than some fixed real number is a finite set.*

*Proof.* Let $M \in \mathbb{R}$ be a constant. Since the height takes values in $\mathbb{Z}^{\geq 1}$ we have:

$$\{x \in \mathbb{Q} : H(x) \leq M\} = \{x \in \mathbb{Q} : H(x) \leq max\{0, \lfloor M \rfloor\}\}.$$

By replacing $M$ with $max\{0, \lfloor M \rfloor\}$ we may assume $M \in \mathbb{Z}^{\geq 0}$ . Take any $x = m/n \in \mathbb{Q}$ with height $H(x) = \max\{|m|, |n|\} \leq M$. It follows that there are only finitely many possibilities for $m$ and $n$. Actually, if we assume $n \geq 1$ we have $\leq M$ possibilities for $n$ and $2M + 1$ possibilities for $m$. It follows that

$$|\{x \in \mathbb{Q} : H(x) \leq M\}| \leq 2M^2 + M.$$

We conclude, that there are only finitely many $x = m/n$ with $H(x) \leq M$. □

*Proof of lemma 2.1.* Fix a real number $M$.

$$\{P \in C(\mathbb{Q}) : h(P) \leq M\} = \{P \in C(\mathbb{Q}) : H(P) \leq e^M\}$$

We can use the finiteness property of the height. This means that there are only finitely many possibilities for the $x$-coordinate of $P$ and for each $x$-coordinate there are only two possibilities for the $y$-coordinate. □

## Lemma 2: Height of $P + P_0$

**Lemma 2.2.** *Let $P_0$ be a fixed rational point of $C$. There is a constant $\kappa_0$ that depends on $P_0$ and on $a, b, c$, so that*

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

*for all $P \in C(\mathbb{Q})$.*

To prove this lemma, we need two preliminary results.

**Result 2.2.** *If $P = (x, y) \in C(\mathbb{Q})$ then $x$ and $y$ have the form*

$$x = \frac{m}{e^2}, y = \frac{n}{e^3}$$

*for integers $m, n, e$ with $e > 0$ and $gcd(m, e) = gcd(n, e) = 1$.*

*Proof.* Write

$$x = \frac{m}{M} \text{ and } y = \frac{n}{N}$$

in lowest terms with $M > 0$ and $N > 0$. Substituting into the equation of the curve gives

$$\frac{n^2}{N^2} = y^2 = x^3 + ax^2 + bx + c = \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M} + c$$

$$\Leftrightarrow M^3n^2 = N^2m^3 + aN^2Mm^2 + bN^2M^2m + cN^2M^3.$$

Step 1: We can write $M^3n^2 = N^2(m^3 + aMm^2 + bM^2m + cM^3)$. Hence, $N^2|M^3n^2$ but since $N$ and $n$ are coprime $N^2|M^3$.

Step 2: Rearranging gives

$$M^3n^2 - (aN^2Mm^2 + bN^2M^2m + cN^2M^3) = N^2m^3. \tag{1}$$

$$M(M^2n^2 - (aN^2m^2 + bN^2Mm + cN^2M^2)) = N^2m^3.$$

Therefore, $M|N^2m^3$ and since $M, m$ are coprime, we find that $M|N^2$.

Step 3: This implies that

$$M^2(Mn^2 - (a\frac{N^2}{M}m^2 + bN^2m + cN^2M) = N^2m^3.$$

So, $M^2|N^2m^3 \Rightarrow M^2|N^2$ using again $\gcd(M, m) = 1$. Thus, $M|N$.

Step 4: Using a similar argument as in Step 3 and again equation (1), we get $M^3|N^2$

From $N^2|M^3$ (step 2) and $M^3|N^2$ (step 2) and $M, N > 0$ it immediately follows that $M^3 = N^2$. In step 2 we have shown that $M|N$ so if we take $e := N/M$, we get that

$$e^2 = \frac{N^2}{M^2} = \frac{M^3}{M^2} = M \text{ and } e^3 = \frac{N^3}{M^3} = \frac{N^3}{N^2} = N.$$

We can conclude that $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$. □

The second result relates the height of the $y$-coordinate of a rational point on the curve $f(x)$ to the height of the point.

**Result 2.3.** *There is a constant $K > 0$, depending on $a, b, c$ (here we mean the coefficients of the curve) such that $|n| \leq KH(P)^{3/2}$ for all $P = (\frac{m}{e^2}, \frac{n}{e^3}) \in C(\mathbb{Q})$.*

*Proof.* We multiply

$$(\frac{n}{e^3})^2 = (\frac{m}{e^2})^3 + a(\frac{m}{e^2})^2 + b\frac{m}{e^2} + c$$

by $e^6$ and this yields

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6.$$

using triangle inequality and the fact that $|m| \leq H(P)$ and $e^2 \leq H(P)$ by definition of the height:

$$\Rightarrow |n^2| \leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6| \leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3$$

The result follows by taking $K = \sqrt{1 + |a| + |b| + |c|}$. □

We are now ready to prove lemma 2.2.

*Proof of lemma 2.2.* The idea is to write out the formula for the sum of two points and to use the triangle inequality. If $P_0 = \mathscr{O}$, the result is trivial. Hence, we assume that $P_0 = (x_0, y_0) \neq \mathscr{O}$. It is enough to prove the inequality for all $P$ except for some finite points (we just consider the differences $h(P + P_0) - 2h(P)$ and take $\kappa_0$ larger than the finite number of values that occur). We want to avoid using the duplication formula (see first talk). Therefore, we may assume $P \notin \{P_0, -P_0, \mathscr{O}\}$. We write

$$P = (x, y) \text{ and } P + P_0 = (\xi, \mu).$$

We want to express the height of $P + P_0$ in terms of $(x, y)$ and $x_0, y_0$. From the first talk we know that

$$\xi + x + x_0 = \lambda^2 - a \text{ with } \lambda = \frac{y - y_0}{x - x_0}.$$

Substituting $\lambda$ gives us

$$\xi = \frac{(y - y_0)^2}{(x - x_0)^2} - a - x - x_0 = \frac{(y - y_0)^2 - (x - x_0)^2(x + x_0 + a)}{(x - x_0)^2}.$$

After some manipulation one can see that $y^2 - x^3$ appears in the numerator and can be replaced by $ax^2 + bx + c$ since $P$ lies on the curve. Hence, there exist rational numbers $A, B, C, D, E, F, G \in \mathbb{Q}$ that can be expressed in terms of $a, b, c$ and $(x_0, y_0)$ so that

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}.$$

We may assume that $A, B, C, D, E, F, G \in \mathbb{Z}$ after multiplying the numerator and denominator by the least common multiple of the denominators of $A, B \dots G$. Note that it is okay for our constant $\kappa_0$ to depend on $A, B, \dots G$ since they only depend on $a, b, c, P_0$. Using result 2.2, we write $x = m/e^2$ and $y = n/e^3$ and multiply denominator and numerator by $e^4$.

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

We have achieved that the numerator and denominator are both integers. It might not be in lowest terms, but cancellation will only make the height smaller.

$$H(\xi) \leq \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}.$$

By definition, $|e| \leq H(P)^{1/2}$ and $|m| \leq H(P)$ and by result 2.3, $|n| \leq KH(P)^{3/2}$. Here, $K$ is a constant that only depends on $a, b, c$. Now we apply the triangle inequality and this gives

$$|Ane + Bm^2 + Cme^2 + De^4| \leq |Ane| + |Bm^2| + |Cme^2| + |De^4| \leq (|AK| + |B| + |C| + |D|)H(P)^2.$$

and

$$|Em^2 + Fme^2 + Ge^4| \leq |Em^2| + |Fme^2| + |Ge^4| \leq (|E| + |F| + |G|)H(P)^2.$$

In summary,

$$H(P+P_0) = H(\xi) \leq \max\{|AK|+|B|+|C|+|D|, |E|+|F|+|G|\}H(P)^2.$$

Finally, taking the logarithm we get that

$$h(P+P_0) \leq 2h(P) + \kappa_0.$$

where $\kappa_0 = \log \max\{|AK|+|B|+|C|+|D|, |E|+|F|+|G|\}$ is a constant depending only on $a, b, c$ and $P_0$. This is what we wanted to prove. □

# 3 Lemma 3: Height of 2P

In this section, we want to prove that

**Lemma 3.1.** *There is a constant $\kappa$ depending on $a, b, c$ s.t*

$$h(2P) \geq 4h(P) - \kappa \quad \textit{for all } P \in C(\mathbb{Q})$$

*Proof of lemma 3.1.* Let $P \in C(\mathbb{Q})$.
Write $P = (x, y)$.
Since there are only finitely many points $P \in C(\mathbb{Q})$ such that $2P = 0$, we can suppose $2P \neq 0$.
Therefore we have $f(x) \neq 0$, where $f(x) = x^3 + ax^2 + bx + c$.
From a duplication formula from one of the earlier talks we know that if we write $2P = (\xi, \nu)$ we have

$$\xi + 2x = \frac{f'(x)^2}{4y^2} - a$$

$$\iff \xi = \frac{f'(x)^2 - f(x)(8x+4a)}{4f(x)}$$

Due to the definition of the height of a point $P \in C(\mathbb{Q})$ we have $h(2P) = h(\xi)$ and $h(P) = h(x)$.
Therefore we need to prove that $h(\xi) \geq 4h(x) - \kappa$, where $\kappa$ only depends on the coefficients of $f$.
Since $f$ is non-singular, $f$ and $f'$ have no common root.
Therefore $f'(X)^2 - f(X)(8X+4a)$ and $4f(X)$ have no common roots.

**Lemma 3.2.** *Let $\phi, \psi \in \mathbb{Z}[X]$ with no common complex root.*
*Let $d := max\{deg(\psi), deg(\phi)\}$.*
*Then we have*
*(a) $\exists R \in \mathbb{Z}$ such that for all $n, m \in \mathbb{Z}$ coprime we have that*

$$gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right) \quad \textit{divides} \quad R$$

*(b) There are constants $\kappa_1, \kappa_2 \in \mathbb{R}$ such that for all $n, m \in \mathbb{Z}$ with $\psi\left(\frac{m}{n}\right) \neq 0$, we have*

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2$$

*We will proof this lemma later, for now lets suppose it is true.*

Let $\phi(X) := f'(X)^2 - f(X)(8X + 4a)$ and $\psi(X) := 4f(X)$.
Since $\psi$ and $\phi$ are polynomials in $\mathbb{Z}[X]$ with no common roots, we can apply the lemma 3.2.
Since $deg(f(x)) = 3$, we have $deg(f'(x)^2) = 4$ and therefore $d = \max\{deg(\psi, \phi)\} = 4$.
Using lemma 3.2, we find a constant $\kappa_1$ only dependent on $\psi$ and $\phi$ such that

$$4h(x) - \kappa_1 \leq h\left(\frac{\phi(x)}{\psi(x)}\right) = h(\xi)$$

$$\iff 4h(P) - \kappa_1 \leq h(2P)$$

Since $P$ was arbitrary such that $2P \neq 0$ and this only happens finitely often, we can finally find a constant $\kappa$ such that for all $P \in C(\mathbb{Q})$ we have

$$4h(P) - \kappa \leq h(2P)$$

□

Now we want to prove (a) of lemma 3.2.

*Proof of lemma 3.2 (a).* Since $\phi$ and $\psi$ have no common roots we have $gcd_{\mathbb{Q}[X]}(\psi, \phi) = 1$.
Therefore there are $F, G \in \mathbb{Q}[X]$ s.t

$$\phi(X)F(X) + \psi(X)G(X) = 1 \tag{2}$$

Since $F, G \in \mathbb{Q}[X]$ we can find $A \in \mathbb{Z}$ s.t $AF, AG \in \mathbb{Z}[X]$.
Without loss of generality we have $d = deg(\phi)$.
Moreover we can suppose $d > 0$ since in the case $d = 0$, the lemma follows immediately.
Let $D := max\{deg(F), deg(G)\}$.
Let $m, n \in \mathbb{Z}$ coprime.
Multiplying (2) by $An^{D+d}$ and evaluating at $X = \frac{m}{n}$ leads to

$$An^{D+d}\phi\left(\frac{m}{n}\right)F\left(\frac{m}{n}\right) + An^{D+d}\psi\left(\frac{m}{n}\right)G\left(\frac{m}{n}\right) = An^{D+d} \tag{3}$$

To ease notation we define $\Phi := n^d\phi\left(\frac{m}{n}\right)$ and $\Psi := n^d\psi\left(\frac{m}{n}\right)$.
Notice that $\Phi, \Psi \in \mathbb{Z}$.
Let $\gamma := gcd(\Phi, \Psi)$.
Since $\gamma|\Phi$ and $\gamma|\Psi$, it follows from (3) that $\gamma|An^{D+d}$.

*Now we want to find $R \in \mathbb{Z}$ which does not depend on $n, m$ such that $\gamma|R$ to finish the proof of (a).*

**Claim:** $\gamma | A a_d^{D+d}$ where $a_d$ is the leading coefficient of $\phi$.
**Proof of the claim:**
By the definitions we have

$$An^{D+d-1}\Phi = An^{D+d-1}m^d a_d + An^{D+d}m^{d-1}a_{d-1} + .... + An^{D+2d-1}a_0 \tag{4}$$

Since $\gamma | An^{D+d}$ and $\gamma | \Phi$, by (4), we have $\gamma | An^{D+d-1}m^d a_d$.
Therefore

$$\gamma | gcd(An^{D+d}, An^{D+d-1}m^d a_d) \tag{5}$$

Since $gcd(An^{D+d}, An^{D+d-1}m^d a_d) = An^{D+d-1}gcd(n, m^d a_d)$ and $n, m$ are coprime, we have

$$\gamma | An^{D+d-1}a_d$$

Repeating the above by looking at $An^{D+d-2}a_d\Phi$, we find $\gamma | An^{D+d-2}a_d^2$.
This can be repeated until we have $\gamma | A a_d^{d+D}$.

Because $A a_d^{D+d}$ doesn't depend on $n, m$ (a) is proven with $R := A a_d^{D+d}$.

□

Now we want to prove part $(b)$ of lemma 3.2.
Intuitively, $\kappa_1$ and $\kappa_2$ exist because from (a) we know that there are no massive cancellations in the fraction $\left(\frac{\phi(m/n)}{\psi(m/n)}\right)$. This means that $h\left(\frac{m}{n}\right)$ and $h\left(\frac{\phi(m/n)}{\psi(m/n)}\right)$ grow somewhat similar.
We only prove the lower bound, since the upper bound can be proven like lemma 2.

*Proof of the lower bound of (b).* Let $n, m \in \mathbb{Z}$ such that $\psi\left(\frac{m}{n}\right) \neq 0$.
Since $\phi(x) = 0$ only happens finitely often, we can suppose that $\phi\left(\frac{m}{n}\right) \neq 0$.
Let $\xi := \frac{\phi(m,n)}{\psi(m,n)}$.
Since $h(\xi) = h(1/\xi)$, we can assume without loss of generality that $d = deg(\phi)$.
Define $\Phi$ and $\Psi$ as in (a), therefore $\xi = \frac{\Phi}{\Psi}$.
By (a) there exists $R \in \mathbb{N}$, not dependent on $m, n$, such that $gcd(\Psi, \Phi) | R$.
Since $gcd(|\Phi|, |\Psi|) \leq R$, we have

$$H(\xi) \geq \frac{1}{R}\max\{|\Phi|, |\Psi|\}$$

Since $\max\{a, b\} \geq \frac{a+b}{2}$ and by the definition of $\Psi$ and $\Phi$, we have

$$H(\xi) \geq \frac{1}{2R}(|\Phi(m,n)| + |\Psi(m,n)|) = \frac{1}{2R}(|n^d\phi\left(\frac{m}{n}\right)| + |n^d\psi\left(\frac{m}{n}\right)|)$$

Since $H(m/n)^d = \max\{|n|^d, |m|^d\}$ we have

$$\frac{H(\xi)}{H(m/n)^d} \geq \frac{1}{2R}\frac{|n^d\phi\left(\frac{m}{n}\right)| + |n^d\psi\left(\frac{m}{n}\right)|}{\max\{|n|^d, |m|^d\}} = \frac{1}{2R}\frac{|\phi\left(\frac{m}{n}\right)| + |\psi\left(\frac{m}{n}\right)|}{\max\{\frac{|m|^d}{|n|^d}, 1\}} \tag{6}$$

Let $f : \mathbb{R} \to \mathbb{R}$ with $t \mapsto \frac{1}{2R} \frac{|\phi(t)|+|\psi(t)|}{\max\{|t|^d,1\}}$.
Since $\phi$ is of degree $d$ and $\psi$ of degree less or equal to $d$ we have

$$\lim_{|t|\to\infty} f(t) \in \{\frac{|a_d|}{2R}, \frac{|a_d|+|b|}{2R}\}$$

where $a_d$ and $b$ are the leading coefficients of $\phi$ and $\psi$ respectively.
Therefore there exists $t_0 > 0$ such that for any $|t| \geq t_0$ we have $f(t) \geq C$ for some $C > 0$.
Moreover, since $f|_{[-t_0,t_0]}$ is continues on a compact interval, $f$ admits a minima $M$.
Since $\psi$ and $\phi$ have no common roots by assumption, we have $M > 0$.
Therefore $f(t) \geq \min\{M, C\} > 0$ for any $t \in \mathbb{R}$.
Therefore by (6) we have

$$\min\{M, C\} H\left(\frac{m}{n}\right)^d \leq H(\xi)$$

Setting $\kappa_1 := log(2R/min\{M, C\})$ and taking the logarithm, we obtain

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h(\xi)$$

which concludes the proof of the lower bound in (b) since $\xi = \frac{\phi(m/n)}{\psi(m/n)}$.

□

# References


[1] J.H. Silverman and J.T. Tate, *Rational points on elliptic curves*, second edition, *Undergraduate Texts in Mathematics*, Springer, (2015)