Heights

Pia Herkenrath, Ana Pavlaković

13th October, 2020

Our main reference is [1] and we encourage anyone interested in the topic to read the book.

1 Introduction to Heights

Definition 1. Let $x = \frac{m}{n}$ be a rational number in lowest terms. The *height of* x is defined as

$$H(x) = H\left(\frac{m}{n}\right) = \max\{|m|, |n|\}.$$

Remark. The height measures the "complexity" of a given number from a number theoretical point of view. We define this new notion because other (already well-known) measures, like the absolute value, do not suffice. Take, for example, the rational numbers $\frac{1}{2}$ and $\frac{99{,}999}{20{,}000}$. Their absolute values are very close together. But $H(\frac{1}{2}) = 2$ and $H(\frac{99{,}999}{20{,}000}) = 20,000$, which more accurately reflects the complexity of the two numbers.

Another useful property of the height is given in the following statement:

Finiteness Property. *The set of all rational numbers whose height is less than some fixed constant d is finite.*

Proof. Let x be a rational number. Write $x = \frac{m}{n}$. If the height of x is less than some fixed constant d, then by the definition of height both $|m| < d$ and $|n| < d$. This leaves us with only finitely many possibilities for m and n. Hence there are finitely many x with height less than d. Q.E.D

Definition 2. Consider a non-singular cubic curve C given in Weierstrass normal form

$$y^2 = x^3 + ax^2 + bx + c, \tag{1}$$

where a, b, and c are integer coefficients. Let $P = (x, y)$ be a rational point on the curve. Then the *height of* P is defined to be the height of the x-coordinate of P

$$H(P) = H(x).$$

By convention, we set $H(\mathcal{O}) = 1$.

Remark. It makes sense that the height of a point P only depends on its x-coordinate, since $|y|$ is uniquely determined by the x-coordinate.

Definition 3. The *small h height* of P is defined as

$$h(P) = \log H(P).$$

Remark. We will later see that the height adheres to certain rules regarding multiplication under the addition law on the curve. This means that the small height gives us a quantity that behaves according to certain additive rules under the addition of points.

Lemma 1. *For every real number M, the set $A := \{P \in C(\mathbb{Q}) \mid h(P) \leq M\}$ is finite.*

Proof. Let $P = (x, y) \in A$. By definition $A = \{P = (x, y) \in C(\mathbb{Q}) \mid h(x) \leq M\}$. There are only finitely many possibilities for the x-coordinate, as it has to be less or equal than M and it is an integer. For each x-coordinate there are only two possibilities for y, as $y^2 = x^3 + ax^2 + bx + c$. So, in total there are finitely many points in A. Q.E.D

2 Height of $P + P_0$

Lemma 2. *Let P_0 be a fixed rational point on C. There exists a constant κ_0 that depends on P_0 and on a, b, and c, such that*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \qquad \forall P \in C(\mathbb{Q}).$$

Before giving the proof of Lemma 2, we will derive two preliminary results that will be needed later.

Result 1. The x- and y-coordinates of any rational point P on the curve can be written in the form

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

where m, n, $e \in \mathbb{Z}$, $e > 0$ and $\gcd(m, e) = \gcd(n, e) = 1$.

Proof. Since P is a rational point, we can write $x = \frac{m}{R}$ and $y = \frac{n}{S}$ for R, $S \in \mathbb{Z}^+$ with $\gcd(m, R) = \gcd(n, S) = 1$, i.e. x and y are in lowest terms. The goal is to find the relation between R and S.
Substituting x and y into the equation of the curve (1) gives

$$\frac{n^2}{S^2} = \frac{m^3}{R^3} + a\frac{m^2}{R^2} + b\frac{m}{R} + c.$$

Multiplying both sides by R^3S^2 gets rid of the denominators

$$R^3 = S^2m^3 + aS^2Rm^3 + bS^2R^2m + cS^2R^3. \tag{2}$$

Notice that S^2 appears in each term on the right-hand side of (2). This means that $S^2 \mid R^3n^2$. But by assumption $\gcd(n, S) = 1$, which implies

$$S^2 \mid R^3. \tag{3}$$

In equation (2) we also see that R appears in each term on the right-hand side, except for the first one. Thus $R \mid S^2m^3$. But again by assumption $\gcd(m, R) = 1$, so it follows that

$$R \mid S^2. \tag{4}$$

This is equivalent to $R^2 \mid S^2R$. Applying that fact to equation (2) again, one can see that $R^2 \mid S^2m^3$, and thus

$$R \mid S. \tag{5}$$

Similarly, using (5) and equation (2) we get $R^3 \mid S^2m^3$, which implies

$$R^3 \mid S^2. \tag{6}$$

From (3) and (6) it follows immediately that $R^3 = S^2$.
Now take $e = \frac{S}{R}$. Then

$$e^2 = \frac{S^2}{R^2} = \frac{R^3}{R^2} = R,$$

$$e^3 = \frac{S^3}{R^3} = \frac{S^3}{S^2} = S.$$

This gives the desired result.

Q.E.D

Result 2. Let $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$ be a rational point on the curve given in lowest terms. Then the height $H(P)$ can be used to give a bound for the x- and y-coordinates of P:

(i) $|m| \leq H(P)$,

(ii) $e \leq H(P)^{\frac{1}{2}}$,

(iii) There exits a constant $K > 0$ depending on a, b, and c such that $|n| \leq KH(P)^{\frac{3}{2}}$.

Proof. By definition, the height of P is given by $H(P) = H\left(\frac{m}{e^2}\right) = \max\{|m|, e^2\}$. It immediately follows that

$$|m| \leq H(P),$$

and

$$e^2 \leq H(P) \implies e \leq H(P)^{\frac{1}{2}}.$$

To show (iii), we begin by substituting $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ into the equation of the curve (1).

$$\frac{n^2}{e^6} = \frac{m^3}{e^6} + a\frac{m^2}{e^4} + b\frac{m}{e^2} + c$$

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

Taking the absolute value on both sides and using the triangle inequality gives

$$\begin{aligned} |n^2| &= |m^3 + ae^2m^2 + be^4m + ce^6| \\ &\leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6|. \end{aligned}$$

Now we can use the bounds for m and e from above:

$$\begin{aligned} |n^2| &\leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3 \\ &= (1 + |a| + |b| + |c|)H(P)^3. \end{aligned}$$

This implies that

$$|n| \leq \sqrt{1 + |a| + |b| + |c|}\; H(P)^{\frac{3}{2}}.$$

Taking $K = \sqrt{1 + |a| + |b| + |c|}$ gives the desired result. Q.E.D

Now we can use these two results to prove Lemma 2.

Proof of Lemma 2. Fix $P_0 = (x_0, y_0)$. The case $P_0 = \mathcal{O}$ is trivial, so we can assume $P_0 \neq \mathcal{O}$. It is enough to show the inequality for all $P \in C(\mathbb{Q})$ except finitely many. This is because for finitely many P we can simply take the difference $h(P+P_0) - 2h(P)$ and choose κ_0 to be greater than all these differences. Hence, assume $P \notin \{P_0, -P_0, \mathcal{O}\}$. Note that by excluding P_0 we can avoid having to use the duplication formula later. The small height of twice a point $h(2P)$ will be discussed further in Lemma 3.
Now let us write $P = (x, y)$ and $P + P_0 = (\mu, \eta)$. We are interested in the small height of $P + P_0$, and since $h(P + P_0) = h(\mu)$ we need to derive an expression for μ.
In an earlier talk we saw the formula for adding two points on a curve

$$\mu + x + x_0 = \lambda^2 - a\ , \qquad \lambda = \frac{y - y_0}{x - x_0}.$$

Note that λ is well-defined, since $P \neq P_0$, i.e. $x \neq x_0$ by assumption.
Rearranging the above formula for μ and substituting in λ gives

$$\begin{aligned}
\mu &= \frac{(y-y_0)^2}{(x-x_0)^2} - a - x - x_0 \\
&= \frac{(y-y_0)^2 - (x-x_0)^2(a+x+x_0)}{(x-x_0)^2} \\
&= \frac{y^2 - 2yy_0 + y_0^2 - (x^2 - 2xx_0 + x_0^2)(a+x+x_0)}{(x-x_0)^2} \\
&= \frac{y^2 - 2yy_0 + y_0^2 - ax^2 - x^3 - x^2x_0 + 2axx_0 + 2x^2x_0 + 2xx_0^2 - ax_0^2 - x_0^2x - x_0^3}{x^2 - 2xx_0 + x_0^2} \\
&= \frac{y^2 - x^3 - 2yy_0 + x^2(x_0 - a) + x(x_0^2 + 2ax_0) + y_0^2 - x_0^3 - ax_0^2}{x^2 - 2xx_0 + x_0^2}.
\end{aligned}$$

From the equation of the curve (1) we get $y^2 - x^3 = ax^2 + bx + c$. Substituting this into the equation above, we get

$$\begin{aligned}
\mu &= \frac{-2yy_0 + x^2x_0 + x(x_0^2 + 2ax_0 + b) + y_0^2 - x_0^3 - ax_0^2 + c}{x^2 - 2xx_0 + x_0^2} \\
&= \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G},
\end{aligned} \tag{7}$$

where we assume A, B, C, D, E, F, and G to be integers (if not, multiply by their least common divisor).
Note that the constant κ_0 we are looking for may depend on A, B, C, D, E, F and G, since $A, ..., G$ depend only on a, b, c and P_0.
Now by Result 1 our arbitrary point P can be written as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$. Substituting this into (7) yields

$$\begin{aligned}
\mu &= \frac{A\frac{n}{e^3} + B\frac{m^2}{e^4} + C\frac{m}{e^2} + D}{E\frac{m^2}{e^4} + F\frac{m}{e^2} + G} \\
&= \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.
\end{aligned}$$

We know that m, n, and e are integers, and saw earlier that $A, ..., G$ are also integers. This means that both the numerator and the denominator of the equation above are integers. Hence μ is rational. However, the definition of the height was given for rational numbers in *lowest terms*. The number μ may not be in lowest terms, but cancelling reduces the size of both the numerator and denominator of a rational number, and thus also reduces the height. Therefore

$$H(P + P_0) = H(\mu) \leq \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}.$$

We will first consider the numerator of μ. Using the triangle inequality gives

$$|Ane + Bm^2 + Cme^2 + De^4| \leq |Ane| + |Bm^2| + |Cme^2| + |De^4|.$$

Now we can use the bounds for $|m|$, $|n|$, and e from Result 2:

$$\begin{aligned}
|Ane + Bm^2 + Cme^2 + De^4| &\leq |AK|H(P)^2 + |B|H(P)^2 + |C|H(P)^2 + |D|H(P)^2 \\
&= (|AK| + |B| + |C| + |D|)H(P)^2.
\end{aligned} \tag{8}$$

Similarly, we can bound the denominator of μ using the triangle inequality and Result 2:

$$\begin{aligned}
|Em^2 + Fme^2 + Ge^4| &\leq |Em^2| + |Fme^2| + |Ge^4| \\
&\leq |E|H(P)^2 + |F|H(P)^2 + |G|H(P)^2 \\
&= (|E| + |F| + |G|)H(P)^2.
\end{aligned} \tag{9}$$

Combining (8) and (9) with the bound for $H(P+P_0)$ yields

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

Let us define $\kappa_0' := \max\{(|AK|+|B|+|C|+|D|), (|E|+|F|+|G|)\}$. To get the small height, we take the logarithm on both sides

$$\begin{aligned} h(P+P_0) &\leq \log(\kappa_0' H(P)^2) \\ &= \log(\kappa_0') + 2h(P). \end{aligned}$$

Setting $\kappa_0 = \log(\kappa_0')$ concludes the proof.

Q.E.D

3 Height of $2P$

Lemma 3. *There is a constant κ, depending on a, b, and c, so that*

$$h(2P) \geq 4h(P) - \kappa \quad \forall P \in C(\mathbb{Q}).$$

Remark. Proving Lemma 3 is harder than Lemma 2, because we need to make sure there is not too much cancellation, i.e. doubling $\frac{1}{2}$ gives us $\frac{2}{2} = 1$, which has smaller height than $\frac{1}{2}$. Luckily, on elliptic curves there is some sort of rule that the height follows with respect to doubling, as stated in Lemma 3.

Proof of Lemma 3. First, note that we can ignore any finite set of points, since we can always take κ larger than $4h(P)$ for all points in that finite set. So, we will discard the finitely many points satisfying $2P = \mathcal{O}$.
Now, we recall the duplication formula which we saw in the first talk: Let $P = (x, y)$ and $2P = (\xi, \eta)$ and denote by $f'(x)$ the derivative $f'(x) = 3x^2 + 2ax + b$ of $f(x) = x^3 + ax^2 + bx + c$ with respect to x. Then we can write

$$\xi + 2x = \lambda^2 - a \qquad \text{where } \lambda = \frac{f'(x)}{2y},$$

that is

$$\xi = \frac{f'(x)^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 + \ldots}{4x^3 + \ldots}.$$

This is well-defined, because as $2P \neq \mathcal{O}$ by assumption, therefore $f(x) \neq 0$. Thus, ξ is the quotient of two polynomials in x with integer coefficients. Since $y^2 = f(x)$ is non-singular, $f(x)$ and $f'(x)$ have no common roots. Hence, $x^4 + \ldots$ and $4x^3 + \ldots$ do not have any common roots. Recall that we want to prove $h(2P) \geq 4h(P) - \kappa$ for some κ that depends solely on a, b, c. In the new notation this is equivalent to:

$$h(\xi) \geq h(x) - \kappa.$$

We introduce a "sublemma" in which we state (and prove) something slightly stronger from which Lemma 3 will immediately follow.
Sublemma. Let $\phi(X)$ and $\psi(X)$ be polynomials with integer coefficients and no common complex roots. Let d denote the maximum degree of ϕ and ψ. Then

(a) there exists a constant $R \geq 1$ depending solely on ϕ and ψ such that for all $\frac{m}{n} \in \mathbb{Q}$:

$$\gcd\left(n^d \phi\left(\frac{m}{n}\right), n^d \psi\left(\frac{m}{n}\right)\right) \;\Big|\; R,$$

and

(b) there exist constants κ_1 and κ_2 depending on ϕ and ψ such that for all $\frac{m}{n} \in \mathbb{Q}$ with $\psi\left(\frac{m}{n}\right) \neq 0$:

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

Proof of Sublemma. We will use part (a) to prove the left inequality of part (b) which implies lemma 3.

(a) First of all, note that taking the greatest common divisor makes sense: Since the degrees of ϕ and ψ are at most d, $n^d\phi(m/n)$ and $n^d\psi(m/n)$ are integers. Therefore

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

is well-defined.
In addition, by potentially switching the roles of ϕ and ψ, we may assume without loss of generality that ϕ has degree d and the degree of ψ is $e \leq d$. We now define

$$\Phi(m,n) := n^d\phi(m/n) = a_0m^d + a_nm^{d-1}n + \ldots + a_dn^d$$
$$\Psi(m,n) := n^d\psi(m/n) = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e+1} + \ldots + b_en^d.$$

Now we move on to the actual proof. Note that as $\phi(X)$ and $\psi(X)$ do not have any common roots, they are relatively prime on $\mathbb{Q}[X]$ and thus generate the unit ideal, i.e. $(\phi) + (\psi) = (1) = \mathbb{Q}[X]$. Therefore, there exist polynomials F, G with rational coefficients such that

$$F(X)\phi(X) + G(X)\psi(X) = 1. \quad (*)$$

Define A to be large enough such that $AF(X)$ and $AG(X)$ have integer coefficients and let $D := \max\{\deg F, \deg G\}$. Remark that A and D do not depend on n and m. If we take $X = \frac{m}{n}$ and multiply $(*)$ by An^{D+d} we get

$$n^DAF\left(\frac{m}{n}\right) \cdot n^d\phi\left(\frac{m}{n}\right) + n^DAG\left(\frac{m}{n}\right) \cdot n^d\psi\left(\frac{m}{n}\right) = An^{D+d}.$$

Observe that $n^DAF(X)$ and $n^DAG(X)$ are integers because $n, D, AF\left(\frac{m}{n}\right)$, and $AG\left(\frac{m}{n}\right)$ are integers. Define $\gamma := \gamma(m,n) := \gcd(\Phi(m,n), \Psi(m,n))$. Then we can conclude that γ divides An^{D+d}. Unfortunately, An^{D+d} depends on n and our R from the sublemma may only depend on ϕ and ψ, so we cannot take $R := An^{D+d}$. Instead, we claim that $\gamma \mid Aa_0^{D+d}$. Indeed, we observe that, as γ divides $\Phi(m,n)$ and $n^{D+d-1} \in \mathbb{Z}$,

$$\gamma \mid An^{D+d-1}\Phi(m,n) = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + \ldots + Aa_dn^{D+2d-1}.$$

Note that on the right-hand side of the equation except for the first term all contain An^{D+d} as a factor. Therefore, γ divides the first term $Aa_0m^dn^{D+d-1}$. As m, n are coprime, $\gamma \mid Aa_0n^{D+d-1}$. If we repeat the above argument using that $\gamma \mid Aa_0n^{D+d-1}\Phi(m,n)$, we can conclude that $\gamma \mid Aa_0^2n^{D+d-2}$. Repeating this multiple times yields:

$$\gamma \mid Aa_0^{D+d}.$$

Defining $R := Aa_0^{D+d}$ we can conclude the proof.

(b) For the proof we use part (a). As only the lower bound is relevant for the proof of Lemma 3, we shall only prove that one, although the upper bound can be proven analogously. As in the previous proofs, we again can exclude a finite set of rational numbers and therefore assume that $\frac{m}{n}$ is not a root of ϕ. Note that if $r \neq 0$, then $h(r) = h\left(\frac{1}{r}\right)$, so without loss of generality we can assume that $\deg\phi = d$ and $\deg\psi = e \leq d$ (otherwise we can reverse the

roles of ϕ and ψ).
We can write

$$\zeta = \frac{\phi(m/n)}{\psi(m/n)} = \frac{n^d\phi(m/n)}{n^d\psi(m/n)} = \frac{\Phi(m,n)}{\Psi(m,n)}.$$

Observe that this is a quotient of integers, because the largest common denominator of $\phi(m/n)$ and $\psi(m/n)$ is n^d.
Assuming that Φ and Ψ do not have common factors we know that

$$H(\zeta) = \max\{|\Phi(m,n)|, |\Psi(m,n)|\}.$$

But if they do have common factors, this becomes an inequality. As this is not a really good estimate, we use part (a) to improve it. By part (a) there exists a constant $R \geq 1$ depending only on ϕ and ψ such that

$$\gcd(\Phi(m,n), \Psi(m,n)) \mid R.$$

With this we have a better estimate for $H(\zeta)$ because we have a bound for the possible cancellation if they have common factors:

$$\begin{aligned} H(\zeta) &\geq \frac{1}{R}\max\{|\Phi(m,n)|, |\Psi(m,n)|\} \\ &= \frac{1}{R}\max\{|n^d\phi(m/n)|, |n^d\psi(m/n)|\} \\ &\geq \frac{1}{2R}\{|n^d\phi(m/n)| + |n^d\psi(m/n)|\}. \end{aligned}$$

In the last inequality we use the general fact that $\max\{a,b\} \geq \frac{1}{2}(a+b)$. We now compare $H(\zeta)$ to $H(m/n)^d := \max\{|m|^d, |n|^d\}$:

$$\frac{H(\zeta)}{H(m/n)^d} \geq \frac{1}{2R}\frac{|n^d\phi(m/n)| + |n^d\psi(m/n)|}{\max\{|m|^d, |n|^d\}} = \frac{1}{2R}\frac{|\phi(m/n)| + |\psi(m/n)|}{\max\{|m/n|^d, 1\}}.$$

Define

$$p(t) := \frac{|\phi(t)| + |\psi(t)|}{\max\{|t|^d, 1\}}.$$

We want to show that there exists a constant $C > 0$ such that $p(t) \geq C$ for all $t \in \mathbb{R}$. For this observe that $\deg\phi = d$ and $\deg\psi \leq d$, so

$$\lim_{|t|\to\infty} p(t) \neq 0.$$

In particular,

$$\lim_{|t|\to\infty} p(t) = \begin{cases} |a_0| & \text{if } \deg\psi < d, \\ |a_0| + |b_0| & \text{if } \deg\psi = d. \end{cases}$$

If we consider some closed interval $I \neq \mathbb{R}$, then we can conclude that p is bounded away from 0 on I. Inside I, as $p(t)$ is continuous we know that $p(t) > 0$ because ϕ, ψ have no common zeros. A continuous function on a compact set such as the closed interval I assumes minimum and maximum values, i.e. $\min_{t\in I} p(t), \max_{t\in I} p(t) > 0$. Therefore there exists such a $C > 0$.
As

$$\frac{H(\zeta)}{H(m/n)^d} \geq \frac{1}{2R}p\left(\frac{m}{n}\right),$$

it follows that $H(\zeta) \geq \frac{C}{2R} \cdot H(m/n)^d$. Hence, we get the inequality

$$h(\zeta) \geq d \cdot h\left(\frac{m}{n}\right) - \kappa_1$$

where $\kappa_1 := \log(2R/C)$, because $h(x) := \log H(x)$. Note that C and R only depend on ϕ and ψ, not on n and m. This concludes the proof of part (b).

Q.E.D

From the left inequality in part (b), Lemma 3 follows directly, with $d = 4$, because $\phi(x) = x^4 + \ldots$ and $\psi(x) = 4x^3 + \ldots$ and therefore,

$$h(\xi) \geq 4h(x) - \kappa \quad \text{for all } x = \frac{m}{n} \text{ that are not roots of } \psi.$$

So,

$$h(2P) \geq 4h(P) - \kappa \quad \forall P \in C(\mathbb{Q}).$$

Furthermore, κ (which we take equal to κ_1 from the sublemma) only depends on ϕ and ψ, i.e. on a, b, and c from the Weierstrass normal form of the elliptic curve. This concludes the proof. Q.E.D

References

[1] J.H. Silverman and J.T. Tate. *Rational Points on Elliptic Curves*. Springer, 1992. ISBN: 978-3-319-18588-0.