The Mordell-Weil Theorem [1]

D.S. Nagaraj and B. Sury

1. Introduction

The first important result on elliptic curves E over number fields K is the theorem of the title. It says that $E(K)$ is a finitely generated abelian group. In other words, $E(K) \cong \mathbb{Z}^r \oplus F$ where F is a finite abelian group, the torsion subgroup. One refers to $E(K)$ as the Mordell-Weil group of E over K. Geometrically, if one is given a system of generators for $E(K)$, then one can produce all the points by the chord and tangent process. This means that one can obtain any point of $E(K)$ by drawing tangents at these points and chords between them, continuing this with the resulting points and repeating this procedure finitely many times. The Mordell-Weil theorem was proved by Mordell for $K = \mathbb{Q}$ and by Weil in general. In the previous chapter, we saw a proof of a weaker statement - the so-called weak Mordell-Weil theorem - which asserts that for any integer m, the group $E(K)/mE(K)$ is finite. To prove the full theorem, one tries to find a 'size' function on $E(K)$ with the following properties:
(i) there are only finitely many elements of a bounded size and,
(ii) for coset representatives $P_1, \ldots, P_r$ in $E(K)$ for the finite group $E(K)/mE(K)$, one can subtract from any element P of $E(K)$, an integral linear combination of the P_i's such that the resulting element is of size bounded by a constant C independently of P.
Once such a size function is produced, it is quite easy to deduce that the P_i's together with the finite set of elements of size at most C generate the Mordell-Weil group $E(K)$. A point to be noted is that there is no known effective way of computing the Mordell-Weil group $E(K)$. The main reason is that there is no known effective way of computing the quotient $E(K)/mE(K)$ for any $m \geq 2$. We partly follow [S] and partly [M] for the proof of the Mordell-Weil theorem.

[1] Elliptic Curves, Modular Forms and Cryptography, *Proceedings of the Advanced Instructional Workshop on Algebraic Number Theory, HRI, Allahabad, 2000* (Eds. A. K. Bhandari, D. S. Nagaraj, B. Ramakrishnan, T. N. Venkataramana), Hindustan Book Agency, New Delhi 2003, pp. 73–84.

2000 *Mathematics subject classification.* Primary: 11G05, 14K15, 14G25.

2. Heights on projective spaces

The 'size' we talked about is encrypted in the notion of the height of a point in $E(K)$. We shall define the height of a point in $\mathbb{P}^n(K)$. Following that, we shall define the height of a point on an elliptic curve by means of a morphism to $\mathbb{P}^1$. The height function on $\mathbb{P}^2$ also proves useful in deducing how the height of points an elliptic curve behaves under its group law. We start with $\mathbb{Q}$ first. For any point P in the projective space $\mathbb{P}^n(\mathbb{Q})$, one can find homogeneous co-ordinates $[x_0 : \cdots : x_n]$ where x_i are integers with no factor common to all of them. This co-ordinate is unique up to changing the sign throughout. One defines the *height* of P as $h(P) = \log \max\{|x_i|; 0 \leq i \leq n\}$. *It is clear that there are only finitely many points in the projective space which have height bounded by any constant.* Note that we have used the property that $\mathbb{Z}$ is a PID to produce homogeneous co-ordinates which are coprime integers. This property does not hold in general for rings of integers in number fields and thus we take another approach which will take care of general number fields also. If a point $P \in \mathbb{P}^n(\mathbb{Q})$ is given in some homogeneous co-ordinates $[x_0 : \cdots : x_n]$ (not necessarily the coprime integral co-ordinates as above), then one can express the height in terms of the x_i's in the following manner:

$$h(P) = \log \max\{|x_i|; 0 \leq i \leq n\} + \sum_{p \ prime} \log \max\{|x_i|_p; 0 \leq i \leq n\}.$$

Here $|x|_p$ denotes the normalized p-adic absolute value defined on any non-zero rational number $x = p^n a/b$ to be p^{-n} where $(p, ab) = 1$. The fact that the definition does not change when the homogeneous co-ordinates are multiplied by any $t \in \mathbb{Q}^*$, is a consequence of the product formula $|t| \prod_p |t|_p = 1$ or, equivalently, of the fundamental theorem of arithmetic. Starting from this definition of height on $\mathbb{P}^n(\mathbb{Q})$, one can define a height function on $E(\mathbb{Q})$ for an elliptic curve E over $\mathbb{Q}$. It is possible to do explicit computations then and prove the Mordell-Weil theorem over $\mathbb{Q}$. However, we develop the basic theory of heights and prove the Mordell-Weil theorem for general number fields.

Let K be a number field and V_K, its set of places. Recall that any nonarchimedean place v of K corresponds to a prime ideal P of the ring of integers $\mathcal{O}_K$ of K and there is a prime number $p \in \mathbb{Z}$ such that $P \cap \mathbb{Z} = p\mathbb{Z}$. Further, the absolute value v is normalized by putting $|p|_v = |p|_p = 1/p$. Let K_v be the completion of K with respect to v, one denotes by n_v, the degree $[K_v : \mathbb{Q}_p]$ for nonarchimedean $v \in V_K$. For archimedean places v in V_K, $K_v = \mathbb{C}$ or $\mathbb{R}$ and let us write $n_v = [K_v : \mathbb{R}]$. The product law on K is then the statement that

$$\prod_v |x|_v^{n_v} = 1 \quad \text{for} \quad x \in K^*.$$

For a number field $L \supset K$, the number n_v for places of K and the numbers n_w for places of L lying above v are related by $\sum_w n_w = [L : K]n_v$ where the sum is over all places of L which lie over v. For $P \in \mathbb{P}^n(K)$ with homogeneous co-ordinates $[x_0 : \cdots : x_n]$.
With these notations, we define :

Definition 1. the *height of P relative to K* is defined as

$$h_K(P) = \sum_{v \in V_K} n_v \log \max\{|x_i|_v ; 0 \le i \le n\}.$$

Lemma 1. (a) *Let $P \in \mathbb{P}^n(K)$. Then, $h_K(P)$ is independent of the choice of the homogeneous co-ordinates.*
(b) *Let $P \in \mathbb{P}^n(K)$. Then, $h_K(P) \ge 0$.*
(c) *For a number field $L \supset K$, and a point $P \in \mathbb{P}^n(K)$, we have $h_L(P) = [L : K]h_K(P)$.*
(d) $\frac{h_K(P)}{[K:\mathbb{Q}]}$ *does not depend on the choice of the field K in which the homogeneous co-ordinates of P lie. In other words, if $\bar{\mathbb{Q}}$ denotes an algebraic closure of $\mathbb{Q}$, then for any $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$ and any number field K such that $P \in \mathbb{P}^n(K)$, the absolute height $h(P) := \frac{h_K(P)}{[K:\mathbb{Q}]}$ is defined independently of K.*
(e) *The absolute height satisfies $h(P) = h(P^\sigma)$ for any $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$ and any $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ where $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ is the group of all field automorphisms of $\bar{\mathbb{Q}}$ which are identity on $\mathbb{Q}$.*

Proof: As mentioned above for $\mathbb{Q}$, (a) is a consequence of the product law on K.
To show (b), note that one can choose one of the homogeneous co-ordinates of P to be 1. Then, every term in the sum defining $h_K(P)$ is non-negative.
(c) follows as an application of the fact noted above that $\sum_w n_w = [L : K]n_v$ where the sum is over all places of L which lie over v.
(d) is an immediate consequence of (c).
To prove (e), note that if $P \in \mathbb{P}^n(K)$, then σ identifies the sets V_K and V_{K^σ} by $|x|_v = |x^\sigma|_{v^\sigma}$ for $x \in K$. As $n_v = n_{v^\sigma}$, it follows that $h_K(P) = h_{K^\sigma}(P^\sigma)$.

It is clear from the definition of height that when $K = \mathbb{Q}$, just looking at the archimedean place shows us that there are only many finitely points of bounded height. We would like to prove this for general K too. For this, it is convenient to use the absolute height. For any point $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$, we shall denote by $\mathbb{Q}(P)$ the minimal field of definition of P; if $[x_0 : \cdots : x_n]$ are homogeneous co-ordinates for P with $x_0 \neq 0$ say, then $\mathbb{Q}(P) = \mathbb{Q}(x_1/x_0, \ldots, x_n/x_0)$. One calls the degree of this extension over $\mathbb{Q}$ to be the degree of P.

Proposition 1. *For any $C, D > 0$, the set*

$$\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) : h(P) \leq C, [\mathbb{Q}(P) : \mathbb{Q}] \leq D\}$$

is finite. In particular, for any number field K, the set $\{P \in \mathbb{P}^n(K) : h(P) \leq C\}$ is finite for every $C > 0$.

Proof: Let us reduce the assertion from $\bar{\mathbb{Q}}$ to $\mathbb{Q}$. Consider the set of points $[x_0 : \cdots : x_n]$ whose degree equals d. For any such point P, we shall associate a point of the projective space $\mathbb{P}^N(\mathbb{Q})$ where $N = \binom{n+d}{d} - 1$ and then show that the set of points of degree d, with height bounded by some constant map in a finite-to-one manner into a set of points of $\mathbb{P}^N(\mathbb{Q})$ whose heights are bounded by some other constant. Let $S_d \subset \mathbb{P}^n(\bar{\mathbb{Q}})$ be the set of all points of degree d over $\mathbb{Q}$. Consider the map

$$\phi_d : S_d \to \mathbb{P}^N(\mathbb{Q}) \; ; \; P = [x_0 : \cdots : x_n] \mapsto [f_0 : \cdots : f_N]$$

where $\prod_\sigma \sum_{i=0}^n x_i^\sigma T_i = \sum_{i=0}^N f_i X_i$ and T_i are indeterminates and the product is over all embeddings σ of $\mathbb{Q}(P)$ in $\bar{\mathbb{Q}}$ which extend the inclusion of $\mathbb{Q}$. Note that the monomials X_i's form a basis of the vector space of all homogeneous polynomials of degree d in the T_i's. The transformation ϕ_d has finite fibres because only the points $[x_0^\sigma : \cdots : x_n^\sigma]$ map onto the same point that $[x_0 : \cdots : x_n]$ maps to. In this manner, the assertion reduces to $\mathbb{Q}$ once we can show that points of bounded height map to points of bounded height. Let us now prove this. Consider any place v of $K = \mathbb{Q}(P)$. Observe that $\log|x+y|_v \leq \max(\log|x|_v, \log|y|_v) + c_v$ for all $x, y \in K$, where c_v can be taken to be 0 for nonarchimedean v and $\log 2$ for archimedean v. Using this, it follows that for each place $v \in V_K$,

$$\max_{0\leq i\leq N} \log|f_i|_v \leq d \; \max_\sigma \max_{0\leq i\leq n} \log|x_i^\sigma|_{v^\sigma} + d_v,$$

for some d_v which can be taken to be zero for nonarchimedean v. Thus, we get

$$h([f_0 : \cdots : f_N]) \leq d_1 h([x_0 : \cdots : x_n]) + d_2$$

for some constants d_1, d_2 which can be computed in terms of n and the degree d of P. This proves that points in $\mathbb{P}^n(\bar{\mathbb{Q}})$ of a given degree and height bounded by some constant map to points in $\mathbb{P}^N(\mathbb{Q})$ of height bounded by some other constant. This latter set we know, is finite. The proposition is proved.

3. Heights on elliptic curves

Our aim now is to define a height function on an elliptic curve E over a field number field K and study its behaviour under the addition law. Note that $E \subset \mathbb{P}^2_K$ is given by the equation $Y^2Z = X^3 + AXZ^2 + BZ^3$.

Definition 2. The *height function of an elliptic curve* E over a number field K is the function $h_E : E(\bar{\mathbb{Q}}) \to \mathbb{R}$; $P \mapsto h(x(P))$ where $x(P)$ is the x-coordinate function in $\mathbb{P}^2(\bar{\mathbb{Q}})$. An analogous definition can be given for any non constant rational function $f \in \bar{\mathbb{Q}}(E)$ but we do not need it here.
As $P \mapsto x(P)$ is a finite-to-one map, we immediately obtain :

Corollary 1. *For any $C > 0$, the set*

$$\{P \in E(K) : h_E(P) \leq C\}$$

is finite.

The main properties of the height function are exhibited in the following result :

Theorem 1. *Let E be an elliptic curve over a number field K. Then, for all $P, Q \in E(K)$,*

$$h_E(P+Q) + h_E(P-Q) = 2h_E(P) + 2h_E(Q) + O(1)$$

where the constant does not depend on the points P, Q.

Remarks 1.
(a) Note that if $P = Q$ in the theorem, then $h_E([2]P) = 4h_E(P) + O(1)$. More generally, for any $n \in \mathbb{Z}$, one can show by induction using the above theorem that $h_E([n]P) = n^2 h_E(P) + O(1)$. Here, for a natural number n, $[n]P$ denotes $P + \cdots + P$ added n times and $[-n]P = (-P) + \cdots + (-P)$ added n times in the group law in E. It turns out (although we do not go into it) that there is a canonical height called the Neron-Tate height which is indeed a quadratic form.

(b) Evidently, the theorem involves writing the x co-ordinates of $P+Q$, $P-Q$ etc. and we are led to some morphisms on $\mathbb{P}^2$ under which we need to know how the height changes. This will be a result of independent interest which will also prove the theorem.

Before studying the behaviour of height under morphisms, we show how the main theorem of the article follows from the above theorem.

Mordell-Weil Theorem. *If E is an elliptic curve over an algebraic number field K, then $E(K)$ is a finitely generated abelian group.*

Proof: We shall use the weak Mordell-Weil theorem only for $m = 2$ i.e, we have $E(K)/2E(K)$ is finite. We observe:
(i) For $Q \in E(K)$, there is a constant C_1, depending only on E and the point Q such that for every $P \in E(K)$, we have $h_E(P+Q) \leq 2h_E(P)+C_1$. This is from the previous theorem since the height function is nonnegative.
(ii) There is a constant C_2 depending on E such that for every $P \in E(K)$, we have $h_E([2]P) \geq 4h_E(P) - C_2$. This is simply by taking $P = Q$ in the previous theorem.
(iii) We have already observed that for any $C_3 > 0$, the set $\{P \in E(K) : h_E(P) \leq C_3\}$ is finite.
From these 3 observations and the fact that $E(K)/2E(K)$ is finite, we now prove the theorem. Choose representatives $Q_1, \ldots, Q_r \in E(K)$ for the finite group $E(K)/2E(K)$. Let P be any element of $E(K)$. Write $P = [2]P_1 + Q_{i_1}$ for some $i_1 \leq r$ and some $P_1 \in E(K)$. Continue as $P_1 = [2]P_2 + Q_{i_2}$ etc. At the j-th stage, we have

$$\begin{aligned} h_E(P_j) &\leq \frac{1}{4}(h_E([2]P_j) + C_2) \\ &= \frac{1}{4}(h_E(P_{j-1} - Q_{i_j}) + C_2) \\ &\leq \frac{1}{4}(2h_E(P_{j-1}) + C_1' + C_2), \end{aligned}$$

where C_1' is the maximum of the constants in the observation (i) above with $Q = -Q_1, \ldots, -Q_r$.
Now, we start with P_n for any n and apply the above inequality repeatedly to obtain

$$h_E(P_n) \leq \frac{1}{2^n} h_E(P) + \sum_{k=1}^{n} \frac{2^{k-1}}{2^{2k}}(C_1' + C_2)$$

$$\leq \frac{1}{2^n} h_E(P) + \frac{1}{2}(C_1' + C_2) \leq 1 + \frac{1}{2}(C_1' + C_2)$$

for large enough n depending on P. As $P = [2^n]P_n + \sum_{j=1}^{n} 2^{j-1} Q_{i_j}$, it follows that the finite set

$$\{Q_1, \ldots, Q_r\} \cup \{Q \in E(K) : h_E(Q) \leq 1 + \frac{1}{2}(C_1' + C_2)\}$$

generates $E(K)$. This proves the theorem.

We are left with proving the previous theorem for which we recall the following definition from chapter 1 :

Definition 3. A map $F : \mathbb{P}^n \longrightarrow \mathbb{P}^m$ defined by $F(P) = [f_0(P) : \cdots : f_m(P)]$ where $f_i \in \bar{\mathbb{Q}}[X_0, \ldots, X_n]$ are homogeneous polynomials of degree d with no common nontrivial zero in $\bar{\mathbb{Q}}$ is said to be *a morphism of degree* d. If the polynomials f_i can be chosen to have coefficients in a subfield K of $\bar{\mathbb{Q}}$, then F is said to be defined over K.

For the theorem that we are trying to prove, we need to find out how the height changes under a certain morphism of degree 2. We put this as a general result.

Theorem 2. *Let $F : \mathbb{P}^n \to \mathbb{P}^m$ be a morphism of degree d. Then, there are constants C_1 and C_2 depending on F such that for any $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$, we have*

$$C_1 + dh(P) \leq h(F(P)) \leq C_2 + dh(P).$$

Proof: Let $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(\bar{\mathbb{Q}})$ look at a number field K which contains all the x_i's as well as all the coefficients of the f_i's which define F. For any place v of K, let us define

$$|P|_v = \max_{i \leq n} |x_i|_v \ , \quad |F(P)|_v = \max_{j \leq m} |f_j(P)|_v$$

and $|F|_v = \max\{|a|_v : a \text{ is coefficient of some } f_j\}$. Then, by definition,

$$h(P) = \sum_{v \in V_K} n_v \log |P|_v \ , \quad h(F(P)) = \sum_{v \in V_K} n_v \log |F(P)|_v.$$

We shall first prove the upper bound; this does not need the assumption that the f_i's have no nontrivial common zero. We denote by ϵ_v either 1 or 0 according as whether v is archimedean or not. The notational advantage is that the triangle inequality can be uniformly expressed as

$$|x_1 + \cdots + x_n|_v \leq n^{\epsilon_v} \max\{|x_1|_v, \ldots, |x_n|_v\}.$$

Then, clearly $|f_i(P)|_v \leq C_1^{\epsilon_v}|F|_v|P|_v^d$ for each place v since f_i is homogeneous of degree d. One can take C_1 to be the number of monomials in f_i - this is at the most $\binom{n+d}{d}$. Using this for each f_i, we get $|F(P)|_v \leq C_1^{\epsilon_v}|F|_v|P|_v^d$. This gives us $h(F(P)) \leq \log C_1 + \sum_v n_v \log|F|_v + dh(P)$ as $\sum_v \epsilon_v n_v = [K : \mathbb{Q}]$. This proves the upper bound.
To obtain the lower bound, note that by Hilbert's Nullstellensatz, the ideal generated by $f_0, \ldots, f_m$ in $\bar{\mathbb{Q}}[X_0, \ldots, X_n]$ contains a power of each X_i as the f_i's have no common nontrivial zero. Therefore, for some $e \geq 1$, one can write $X_i^e = \sum_{j=0}^m g_{ij} f_j$ for $i = 0, 1, \ldots, n$ where $g_{ij} \in \bar{\mathbb{Q}}[X_0, \ldots, X_n]$. Now, all the coefficients of all the g_{ij}'s lie in some finite extension of $\mathbb{Q}$ and, we may assume that this is K (by replacing K by a finite extension). Further, one can throw out the parts of each g_{ij} which are not homogeneous of degree $e-d$. In other words, we can assume each g_{ij} is homogeneous of degree $e-d$. Now, since $P = [x_0 : \cdots : x_n]$, we have for each i that $|x_i|_v^e = |\sum_{j=0}^m g_{ij}(P)f_j(P)|_v \leq C_2^{\epsilon_v} \max_j |g_{ij}(P)f_j(P)|_v$. Taking the maximum over i, we get

$$|P|_v^e \leq C_2^{\epsilon_v}|F(P)|_v \max\{|g_{ij}(P)|_v; 0 \leq i \leq n, 0 \leq j \leq m\}.$$

As each g_{ij} is homogeneous of degree $e-d$, the triangle inequality gives

$$|g_{ij}(P)|_v \leq C_3^{\epsilon_v}|G|_v|P|_v^{e-d}.$$

Here, we have denoted by $|G|_v$ the maximum of the v-absolute value of the coefficients of all the g_{ij}'s. Using this in the earlier inequality, we have

$$|P|_v^d \leq C_4^{\epsilon_v}|G|_v|F(P)|_v.$$

As before, if we take logarithms, multiply by n_v and add up, we will obtain the lower bound

$$h(F(P)) \geq \log C_4 + \sum_v n_v \log|G|_v + dh(P).$$

This completes the proof.

Proof of Theorem 1: Let us choose a Weierstrass equation for E over K of the form $y^2 = x^3 + Ax + B$. Let $O \in E(K)$ denote the point at infinity which is the identity element for the group law on $E(K)$. Now, by definition, we have $h_E(O) = 0$ and $h_E(-P) = h_E(P)$ for each $P \in E(K)$. Thus, the result holds if either P or Q is O. Assume now that $P, Q \neq O$. Let us write

$$x(P) = [x_1 : 1]\,,\ x(Q) = [x_2 : 1]\,,\ x(P+Q) = [x_3 : 1]\,,\ x(P-Q) = [x_4 : 1].$$

Here we understand that x_3 (respectively, x_4) is ∞ if $P = -Q$ (respectively, $P = Q$). Note that when $P \neq \pm Q$, we have

$$x_3 = \frac{(y_2 - y_1)^2}{(x_2 - x_1)^2} - x_1 - x_2$$

$$x_4 = \frac{(y_2 + y_1)^2}{(x_2 - x_1)^2} - x_1 - x_2$$

which shows that

$$x_3 + x_4 = \frac{2(x_1 + x_2)(A + x_1x_2) + 4B}{(x_1 + x_2)^2 - 4x_1x_2}$$

$$x_3x_4 = \frac{(x_1x_2 - A)^2 - 4B(x_1 + x_2)}{(x_1 + x_2)^2 - 4x_1x_2}$$

The idea of the proof is now to look at the map which transforms x_1+x_2 and x_1x_2 to $x_3 + x_4$ and x_3x_4 and show that it defines a morphism g of degree 2 on $\mathbb{P}^2$ for which one could apply the previous theorem. In order to define this g, consider the map $\sigma : E \times E \to \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2$ which is the composite of $(P, Q) \mapsto (x(P), x(Q))$ and $([x_1 : y_1], [x_2 : y_2]) \mapsto [y_1y_2, : x_1y_2 + x_2y_1 : x_1x_2]$. If $G : E \times E \to E \times E$ is the map $(P, Q) \mapsto (P + Q, P - Q)$, and $g : \mathbb{P}^2 \to \mathbb{P}^2$ is the map

$$[t : u : v] \mapsto [u^2 - 4tv : 2u(At + v) + 4Bt^2 : (v - At)^2 - 4Btu],$$

then we see that $\sigma \circ G = g \circ \sigma$. Note that the above expression for g is gotten by thinking of t, u, v as $1, x_1 + x_2, x_1x_2$ and of $g([t : u : v])$ as $1, x_3+x_4, x_3x_4$. To verify that g is indeed a morphism, we need to verify that there are no nontrivial common zeroes for the three homogeneous polynomials defining g. Suppose now that $g([t : u : v]) = 0$. If $t = 0$, then evidently $u = v = 0$. So, we may assume that $t \neq 0$. It is convenient to define a new quantity $s = u/2t$ (observe that thinking of t, u, v as $1, x_1 + x_2, x_1x_2$, the equation $u^2 - 4tv = 0$ becomes $x_1 = x_2 = u/2t$ which means that we are dealing with the case $P = \pm Q$.) One can look at the two equations $2u(At + v) + 4Bt^2 = 0 = (v - At)^2 - 4Btu$ and rewrite them in terms of s. We obtain

$$\psi(s) = 4s^3 + 4As + 4B = 0$$

$$\phi(s) = s^4 - 2As^2 - 8Bs + A^2 = 0$$

We need to check whether the polynomials $\phi(X)$ and $\psi(X)$ have common roots. A simple but tedious calculation gives us the identities

$$(12X^2 + 16A)\phi(X) - (3X^3 - 5AX - 27B)\psi(X) = 4(4A^3 + 27B^2).$$

Evidently, the nonsingularity of the Weierstrass equation then shows that $\phi(X)$ and $\psi(X)$ cannot have common roots. Hence g is indeed a morphism on $\mathbb{P}^2$. Therefore, we have

$$h(\sigma \circ G(P,Q)) = h(g \circ \sigma(P,Q)) = 2h(\sigma(P,Q)) + O(1)$$

by theorem 2, as g is a morphism of degree 2 on $\mathbb{P}^2$. If we show that for any $R_1, R_2 \in E(\bar{\mathbb{Q}})$, one has the relation $h(\sigma(R_1, R_2)) = h_E(R_1) + h_E(R_2) + O(1)$, then applying this to both sides of the identity $h(\sigma \circ G(P,Q)) = 2h(\sigma(P,Q)) + O(1)$, the theorem would follow. The claimed relation is evidently valid even without the $O(1)$ term when one of R_1, R_2 is O. Thus, let us assume $R_1 \neq O \neq R_2$. Then, we may write $x(R_i) = [r_i : 1]$ for $i = 1, 2$. Note that

$$\sigma(R_1, R_2) = [1 : r_1 + r_2 : r_1 r_2].$$

Thus, $h_E(\sigma(R_1, R_2)) = h([1 : r_1 + r_2 : r_1 r_2])$ and $h_E(R_1) + h_E(R_2) = h(r_1) + h(r_2)$. The following will then complete the result :

Claim:

$$h(r_1) + h(r_2) - \log 4 \leq h([1 : r_1 + r_2 : r_1 r_2]) \leq h(r_1) + h(r_2) + \log 2.$$

We may restrict to the field $K = \mathbb{Q}(r_1, r_2)$ and prove this for h_K. Note that by the definition of the height function h_K, we need to prove that for each archimedean place v of K, we have the inequalities

$$\begin{aligned} \log\max(|r_1|_v, 1) + \log\max(|r_2|_v, 1) - \log 4 & \\ \leq \ & \log\max(|r_1 + r_2|_v, |r_1 r_2|_v, 1) \\ \leq \ & \log\max(|r_1|_v, 1) + \log\max(|r_2|_v, 1) + \log 2 \end{aligned}$$

and for nonarchimedean places v, the equality

$$\log\max(|r_1|_v, 1) + \log\max(|r_2|_v, 1) = \log\max(|r_1 + r_2|_v, |r_1 r_2|_v, 1).$$

For, once this is done, one can multiply by n_v and add over all v to deduce the claim. Thus, let us fix a place v of K. These inequalities will follow from the triangle inequalities. Let us suppose $|r_1|_v \geq |r_2|_v$

without loss of generality.
Look at a nonarchimedean place v first.
If $|r_1|_v \leq 1$, then clearly

$$\log\max(|r_1|_v, 1) + \log\max(|r_2|_v, 1) = 0 = \log\max(|r_1 + r_2|_v, |r_1 r_2|_v, 1).$$

On the other hand, if $|r_1|_v > 1 \geq |r_2|_v$, then $|r_1 + r_2|_v = |r_1|_v$ so that

$$\begin{aligned} \log\max(|r_1|_v, 1) + \log\max(|r_2|_v, 1) &= \log|r_1|_v \\ &= \log\max(|r_1 + r_2|_v, |r_1 r_2|_v, 1). \end{aligned}$$

Similarly, if $|r_1|_v \geq |r_2|_v > 1$, then

$$\begin{aligned} \log\max(|r_1|_v, 1) + \log\max(|r_2|_v, 1) &= \log|r_1 r_2|_v \\ &= \log\max(|r_1 + r_2|_v, |r_1 r_2|_v, 1). \end{aligned}$$

If v is archimedean, then let us look at the upper bound. This is clear because

$$\begin{aligned} &\log\max(|r_1 + r_2|_v, |r_1 r_2|_v, 1) \\ &\qquad \leq \log 2\max(|r_1|_v, 1) + \log\max(|r_2|_2, 1) \\ &\qquad = \log\max(|r_1|_v, 1) + \log\max(|r_2|_v, 1) + \log 2. \end{aligned}$$

For the lower bound, if $|r_1|_v \leq 2$, then

$$\begin{aligned} &\log\max(|r_1|_v, 1) + \log\max(|r_2|_v, 1) \\ &\qquad \leq 2\log\max(|r_1|_v, 1) \\ &\qquad \leq 2\log 2 \\ &\qquad \leq 2\log 2 + \log\max(|r_1 + r_2|_v, |r_1 r_2|_v, 1). \end{aligned}$$

If $|r_1|_v > 2$, and $|r_2|_v \leq 2$, then we have

$$\begin{aligned} &\log\max(|r_1 + r_2|_v, |r_1 r_2|_v, 1) \\ &\qquad \geq \log\frac{|r_1|_v}{2} = \log|r_1|_v - \log 2 \\ &\qquad \geq \log\max(|r_1|_v, 1) + \log\max(|r_2|_v, 1) - 2\ \log 2. \end{aligned}$$

Finally, if $|r_1|_v \geq |r_2|_v > 2$, then

$$\begin{aligned} &\log\max(|r_1|_v, 1) + \log\max(|r_2|_v, 1) - \log 4 \\ &\qquad = \log|r_1 r_2|_v/4 \leq \log\max(|r_1 + r_2|_v, |r_1 r_2|_v, 1). \end{aligned}$$

Thus, the claim is proved and so is the theorem.

References

[*M*] D. Mumford (with appendices by C.P.Ramanujam and Yu.Manin), *Abelian varieties*, Published for the Tata Institute of Fundamental Research, Bombay by Oxford University Press 1974.

[*S*] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag Graduate Texts in Mathematics **106**, 1986.

(D. S. Nagaraj) Institute of Mathematical Sciences, CIT Campus, Taramani, Chennai 600 113, India.

(B. Sury) Stat-Math Unit, Indian Statistical Institute, Bangalore 560 059, India.

E-mail address, D. S. Nagaraj: `dsn@imsc.res.in`

E-mail address, B.Sury: `sury@isibang.ac.in`