HEIGHTS PROBLEM SET 5

Below you will find some problems to work on for Week 5! There are three categories: beginner, intermediate and advanced.

Beginner problems

The first two questions ask you to adapt the construction of the canonical height function on an elliptic curve to a dynamical setting.

Question 1. Let $f : \mathbb{P}^n \to \mathbb{P}^n$ be a morphism of degree $d \geqslant 2$ defined over a number field K. Recall from lecture that $h(f(P)) = dh(P) + O(1)$ for any $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$, say

$$|h(f(P)) - dh(P)| \leqslant C$$

for any $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Use a telescoping sum argument to show that

$$\left| \frac{h(f^{\circ N}(P))}{d^N} - \frac{h(f^{\circ M}(P))}{d^M} \right| \leqslant \frac{C}{(d-1)d^M}$$

for all $N > M \geqslant 0$. Conclude from this that the function

$$\widehat{h}_f(P) := \lim_{N \to \infty} \frac{h(f^{\circ N}(P))}{d^N}$$

is well-defined, i.e. that the limit always converges.

Question 2. Complete the proof of the following theorem from lecture: let $f : \mathbb{P}^n \to \mathbb{P}^n$ be a morphism of degree $d \geqslant 2$. Then,

(1) $\widehat{h}_f(P) = h(P) + O(1)$ (with big-O constant independent of P)
(2) $\widehat{h}_f(f(P)) = d\widehat{h}_f(P)$.
(3) The function $\widehat{h}_f$ is the unique such function satisfying the above two properties.
(4) $\widehat{h}_f(P) \geqslant 0$ always, and $\widehat{h}_f(P) = 0$ if and only if $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ is pre-periodic (i.e. $f^{\circ N}(P) = f^{\circ M}(P)$ for some distinct $N, M \geqslant 0$).

Question 3. Let K be a number field, and let E/K be an elliptic curve defined over K. Prove that the group $E(K)_{\mathrm{tors}}$ of torsion K-points is finite.

Question 4. Let E be an elliptic curve over a number field K. Show that the next two statements are equivalent.

(a) For all $P, Q \in E(\overline{\mathbb{Q}})$, we have

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

where the implied constants in $O(1)$ depend on E, but are independent of the pair of points P, Q.

(b) For any integer $m \in \mathbb{Z}$, we have

$$h_E(mP) = m^2 h_E(P) + O(1),$$

where the implied constants in the $O(1)$ notation depend only on E and m and not on the point P.

Intermediate problems

Question 5. Let $\alpha_1, \dots, \alpha_n$ be any n algebraic numbers (not necessarily conjugate), and let

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \bar{\mathbb{Q}}[x].$$

Show that

$$-n \log(2) + \sum_{i=1}^{n} h(\alpha_i) \leqslant h([1 : a_1 : \cdots : a_n]) \leqslant (n-1)\log 2 + \sum_{i=1}^{n} h(\alpha_i).$$

Hint: Fix a place v, and use induction on $n = \deg f$ to show that

$$c_v^{-n} \prod_{j=1}^{n} \max\{1, |\alpha_j|_v\} \leqslant \max_{0 \leqslant i \leqslant n} |\alpha_i|_v \leqslant c_v^{n-1} \prod_{j=1}^{n} \max\{1, |\alpha_j|_v\},$$

where $c_v = 1$ if v is non-archimedean, but $c_v = 2$ if v is real, and $c_v = 4$ if v is complex. In the induction step, you'll want to write $f(x) = (x - \alpha_k)g(x)$ with k chosen to maximize $|\alpha_k|_v$.

Advanced problems

Question 6. This problem will give you a way of computing $2 \cdot E(K)$ to use the Descent method for finding $E(K)$. [1] Let E be an elliptic curve defined over K. Consider the ring $R := K[x]/f(x)K[x]$. Define the map $\varphi : E(K) \to R^\times/(R^\times)^2$ given by

$$\varphi(P) = x(P) - x$$

Show the following

(1) φ is a homomorphism
(2) $\ker(\varphi) = 2 \cdot E(K)$

Use the map φ to show that if $E : y^2 = f(x)$ and $f(x) \in \mathbb{Q}[x]$ has three rational roots, then $E(Q)/2E(Q)$ is finite.

Question 7. Let G be an abelian group. Show that G is finitely generated if and only if

(1) G admits a norm (as an abelian group). This is, there is a map $|\cdot| : G \to \mathbb{R}_{\geqslant 0}$ such that
   (i) $\mid mp \mid = \mid m \mid\mid p \mid$ for all $g \in G$ and $m \in \mathbb{Z}$,
   (ii) $\mid h + g \mid \leqslant |h| + |g|$ for all $h, g \in G$,
   (iii) for each $c \in \mathbb{R}$ the set $Gc := \{g \in G \mid |p| \leqslant c\}$ is finite.
(2) G/mG is finite for some integer $m > 1$.

Does your proof determine explicitly a set of generators? Note that this is analogous to the descent method used in the lectures to show that $E(K)$ is finite, where E is an elliptic curve defined over a number field K.

[1] This problem comes from Section 7 of this REU paper