HEIGHTS PROBLEM SET 6

Below you will find some problems to work on for Week 6! There are three categories: beginner, intermediate and advanced.

Beginner problems

Question 1. Let $y^2 = x^3 + Ax + B$ be the defining equation for an elliptic curve E, where A, B are constants in K such that $4A^3 + 27B^2 \neq 0$. Assume that P and Q are points on E such that $x(P) = [x_1 : 1], x(Q) = [x_2 : 1], x(P+Q) = [x_3 : 1]$ and $x(P-Q) = [x_4 : 1]$ (where $x_i = \infty$ if the corresponding point is infinity on $\mathbb{P}^1$). Show that the following identities hold.

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

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

Question 2. Let A and B be elements of K such that $4A^3 + 27B^2 \neq 0$. Let g_0, g_1, g_2 in $K[t,u,v]$ be defined as follows:

$$\begin{aligned} g_0(t,u,v) &:= u^2 - 4tv, \\ g_1(t,u,v) &:= 2u(At+v) + 4Bt^2, \\ g_2(t,u,v) &:= (v - At)^2 - 4Btu. \end{aligned}$$

(a) Show that if $t = 0$, then $u = v = 0$.
(b) Assume $t \neq 0$. Define $z := u/2t$. Using $g_0 = 0$, show that $z^2 = v/t$.
(c) Define $\psi(z) := 4z(A + z^2) + 4B$ and $\varphi(z) := (z^2 - A)^2 - 8Bz$. Show that $g_1(t,u,v) = t^2\psi(z)$ and $g_2(t,u,v) = t^2\varphi(z)$.
(d) Verify that $(12z^2 + 16A)\varphi(z) - (3z^3 - 5Az - 27B)\psi(z) = 4(4A^3 + 27B^2)$.
(e) Conclude that ψ and φ cannot simultaneously vanish, and hence g_0, g_1, g_2 have no common zero with $t \neq 0$.

Conclude that if (t,u,v) is a common zero of g_0, g_1 and g_2, then $t = u = v = 0$.

Question 3. Consider the degree 2 rational map

$$\begin{array}{cccc} F: & \mathbb{P}^2 & \longrightarrow & \mathbb{P}^2 \\ & [x,y,z] & \longmapsto & [x^2, xy, z^2]. \end{array}$$

Note that F above is not a morphism, so Question 6 does not apply to it. Show in fact there are infinitely many points $P \in \mathbb{P}^2(\mathbb{Q})$ such that $h(F(P)) = h(P)$.

Question 4. Let K be a number field, and let E/K be an elliptic curve with canonical height $\widehat{h}_E : E(\overline{\mathbb{Q}}) \to \mathbb{R}$. Consider the pairing

$$\langle P, Q \rangle := \frac{1}{2}\left[\widehat{h}_E(P+Q) - \widehat{h}_E(P) - \widehat{h}_E(Q)\right]$$

on $E(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}})$.

(1) Show that $\langle P, Q \rangle$ is symmetric, bilinear, and satisfies $\langle P, P \rangle = \widehat{h}_E(P)$. The is sometimes called the height pairing on E.
Hint: first show that $\widehat{h}_E$ satisfies an exact parallelogram law.
(2) If you know about tensor products, then show that $\langle -, - \rangle$ extends to a positive definite inner product on the real vector space $E(\overline{\mathbb{Q}}) \otimes_{\mathbb{Z}} \mathbb{R}$.

We will see an application of (a generalization of this) in Question 7.

Intermediate problems

Question 5. In the lecture, Hilbert's Nullstellensatz was used. The most common version of this theorem is given as follows. Let k be an algebraically closed field and consider an ideal $J \subseteq k[X_0, \dots, X_n]$. Define

$$V(J) := \{x \in k^{n+1} \,:\, f(x) = 0 \text{ for all } f \in J\}.$$

The Hilbert Nullstellensatz states that if $f \in k[X_0, \dots, X_n]$ is a polynomial such that $f(x) = 0$ for all $x \in V(J)$, then there must be $e \in \mathbb{Z}_{\geqslant 0}$ such that $f^e \in J$.

Suppose $F\colon \mathbb{P}^N \to \mathbb{P}^M$ is a morphism of degree d over a number field K, i.e.

$$F(P) = [f_0(P)\colon \dots \colon f_M(P)],$$

where the f_i are homogeneous polynomials of degree d in $N+1$ variables with coefficients in K. Assume that the f_i have no common zeros in $\overline{\mathbb{Q}}^{N+1} \backslash (0, 0, \dots, 0)$. Use Hilbert's Nullstellensatz to show that if $[X_0, \dots, X_N]$ are coordinates for $\mathbb{P}^N$, then there is an exponent $e \in \mathbb{Z}_{\geqslant 0}$ and there are polynomials $g_{ij} \in K[x_0, \dots, x_N]$ for $i \in \{0, \dots, N\}$ and $j \in \{0, \dots, M\}$ such that for every $i \in \{0, \dots, N\}$, we have

$$x_i^e = \sum_{j=0}^{M} g_{ij} f_j.$$

Definition 1. For K a number field, v a place of K, and $g \in K[x_0, \dots, x_n]$ a polynomial, we let $|g|_v$ denote the maximal absolute value of any of its coefficients, i.e. if $g = \sum_I a_I x^I$ with I ranging over all multi-indices $(c_0, \dots, c_n) \in \mathbb{Z}_{\geqslant 0}^{n+1}$ with $c_0 + \dots + c_n \leqslant \deg g$,[1] then $|g|_v = \max_I |a_I|_v$.

Question 6. In lecture, we saw that for a morphism $F = [f_0, \dots, f_M] : \mathbb{P}^N \to \mathbb{P}^M$ of degree d over a number field K, one has

$$h(F(P)) = dh(P) + O(1)$$

if the polynomials $f_i \in K[x_0, \dots, x_N]$ have no common zero other than $(x_0, \dots, x_N) = (0, \dots, 0)$. In this exercise, we ask you to go over the steps of this proof, and fill in any details missing from lecture.

(1) Let $g \in K[x_0, \dots, x_N]$ be homogeneous of degree d, and let v be a place of K. If v is archimedean, show that

$$|g(P)|_v \leqslant \binom{N+d}{d} |g|_v \max_{0 \leqslant i \leqslant N} |x_i|_v^d \text{ for all } P = [x_0, \dots, x_N] \in \mathbb{P}^N(\overline{\mathbb{Q}}).$$

If v is non-archimedean, show that

$$|g(P)|_v \leqslant |g|_v \max_{0 \leqslant i \leqslant N} |x_i|_v^d \text{ for all } P = [x_0, \dots, x_N] \in \mathbb{P}^N(\overline{\mathbb{Q}}).$$

Use this to conclude that

$$h(F(P)) \leqslant dh(P) + C_2 \text{ for all } P = [x_0, \dots, x_N] \in \mathbb{P}^N(\overline{\mathbb{Q}}),$$

where $C_2 = [K : \mathbb{Q}] \log \binom{N+d}{d} + h(F)$, where $|F|_v := \max_{0 \leqslant j \leqslant M} |f_j|_v$ and $h(F) := \sum_v \log |F|_v$.[2]

(2) Hilbert's Nullstellsatz (See Question 5) guarantees the existence of an exponent e and polynomials $g_{ij} \in K[x_0, \dots, x_N]$ such that for every $i \in \{0, \dots, N\}$, we have

$$x_i^e = \sum_{j=0}^{M} g_{ij} f_j.$$

[1] Here, $x^I := x_0^{c_0} x_1^{c_1} \dots x_n^{c_n}$ and $a_I \in K$ is just some choice of coefficient associated with I.

[2] This $h(F)$ is the height of the projective point whose coordinates are given by the collection of coefficients of the f_j's

For a place v, let $|G|_v := \max_{i,j} |g_{ij}|_v$. To avoid breaking into archimedean and non-archimedean cases, we now introduce

$$\varepsilon_v := \begin{cases} 1 & \text{if } v \text{ archimedean} \\ 0 & \text{otherwise.} \end{cases}$$

To ease notation even further, for a point $P = [x_0, \ldots, x_N]$ in projective space, we define $|P|_v := \max_{0 \leqslant i \leqslant N} |x_i|_v$. Now, arguing as in (1), show that

$$|P|_v^e \leqslant (M+1)^{\varepsilon_v} \left(\max_{i,j} |g_{ij}(P)|_v \right) |F(P)|_v \leqslant C' |F(P)|_v |P|_v^{e-d} \text{ for any } P \in \mathbb{P}^N(\overline{\mathbb{Q}}),$$

where $C' := (M+1)^{\varepsilon_v} \binom{N+e-d}{N}^{\varepsilon_v} |G|_v$. Use this to conclude that

$$dh(P) + C_1 \leqslant h(F(P)) \text{ for all } P \in \mathbb{P}^N(\overline{\mathbb{Q}}),$$

where $C_1 = [K : \mathbb{Q}] \left(\log(M+1) + \log \binom{N+e-d}{N} \right) + h(G)$, where $h(G) := \sum_v \log |G|_v$.

Advanced problems

Question 7. This question will assume some familiarity with algebraic curves and their jacobians. In addition to the Mordell-Weil Theorem (that the group of rational points on an elliptic curve is finitely generated), another celebrated application of heights is in Vojta's proof of the Mordell Conjecture[3]. This conjecture states that any curve of genus $g \geqslant 2$ defined over a number field K has finitely many K-points. After assuming some hard facts about heights on curves and their jacobians, we will ask you to prove this statement.

Let K be a number field, let C/K be a curve of genus $g \geqslant 2$, and let $J = \mathrm{Jac}(C)$ be its jacobian. Assume that $C(K) \neq \varnothing$, so we may define an Abel-Jacobi embedding $j : C \hookrightarrow J$. We take for granted the following facts.

(1) There exists a height function $\widehat{h} : J(\overline{\mathbb{Q}}) \to \mathbb{R}$ which satisfies both the Northcott property and that $\widehat{h}(mx) = m^2 \widehat{h}(x)$ for any $m \in \mathbb{Z}$ and $x \in J(\overline{\mathbb{Q}})$.[4] In particular, the points of height 0 are exactly the torsion points of J. Furthermore, the map $\langle -, - \rangle : J(\overline{\mathbb{Q}}) \times J(\overline{\mathbb{Q}}) \to \mathbb{R}$ defined by

$$\langle x, y \rangle := \frac{1}{2} \left[\widehat{h}(x+y) - \widehat{h}(x) - \widehat{h}(y) \right]$$

is a symmetric, bilinear pairing satisfying $\langle x, x \rangle = \widehat{h}(x)$. Inspired by this, we introduce the notation

$$\|x\| := \sqrt{\langle x, x \rangle} = \sqrt{\widehat{h}(x)}$$

for $x \in J(\overline{\mathbb{Q}})$.

(2) The group $J(K) \subset J(\overline{\mathbb{Q}})$ of K-points on the jacobian is finitely generated, and the pairing $\langle -, - \rangle$ considered above gives a positive definite inner product on the finite dimensional vector space $V := J(K) \otimes_{\mathbb{Z}} \mathbb{R}$.

[3] This conjecture was originally proved by Faltings.

[4] For those more familiar with the Weil height machinery, on J, there is a so-called theta divisor $\Theta := \underbrace{j(C) + \cdots + j(C)}_{(g-1) \text{ summands}} \subset J$. The function $\widehat{h}$ alluded to here is a canonical version of the height function associated to the divisor $\Theta + [-1]^*\Theta$, where $[-1] : J \to J$ is negation in J's group law.

(3) For any $\varepsilon > 0$, there exists constants $B > 0$ and $\kappa \geqslant 1$ such that for any distinct $P, Q \in C(\overline{\mathbb{Q}})$ satisfying both[5]

$$\|j(P)\| \geqslant \|j(Q)\| > B \text{ and } \frac{\langle j(P), j(Q)\rangle}{\|j(P)\|\|j(Q)\|} \geqslant \frac{3}{4} + \varepsilon,$$

one has

$$\|j(P)\| \leqslant \kappa\|j(Q)\|.$$

This is called Vojta's inequality.

Use the above 3 facts in order to prove that $C(K)$ is finite. Hint: look at the image of $C(K)$ in V, and split V into (finitely many!) cones s.t. any two points in a given cone have a small angle between them.

[5]The constant 3/4 appearing below can actually be replaced with $\sqrt{g}/g$. For an elliptic curve, we have $g = 1$, and so the statement of Vojta's inequality would be useless in that case. This is good because there exists elliptic curves with infinitely many rational points.