HEIGHTS PROBLEM SET 1

Below you will find some problems to work on for Week 1! There are three categories: beginner, intermediate and advanced. The exercises are meant to get a feeling for projective varieties over $\mathbb{Q}$ and heights. Choose the ones that intrigue you! We begin by collecting some useful definitions.

Definition 1. Recall that *projective N-space* over a field K, denoted by $\mathbb{P}^N$ or $\mathbb{P}^N(K)$, is the set of all $(N+1)$-tuples

$$(x_0, \dots, x_N) \in K^{N+1}$$

such that at least one x_i is nonzero, modulo the equivalence relation

$$(x_0, \dots, x_N) \sim (y_0, \dots, y_N)$$

if there exists a $\lambda \in K \backslash \{0\}$ such that $x_i = \lambda y_i$ for all i. An equivalence class

$$\{(\lambda x_0, \dots, \lambda x_N) : \lambda \in K \backslash \{0\}\}$$

is denoted by $[x_0, \dots, x_N]$, and the x_i are called *homogeneous coordinates* for the corresponding point in $\mathbb{P}^N$.

Definition 2. A polynomial $f \in K[X_0, \dots, X_N]$ is *homogeneous of degree d* if

$$f(\lambda X_0, \dots, \lambda X_N) = \lambda^d f(X_0, \dots, X_N) \quad \text{for all } \lambda \in K.$$

Definition 3. A *rational map of degree d* between projective spaces is a map

$$\varphi : \mathbb{P}^N \to \mathbb{P}^M$$
$$\varphi(P) = [f_0(P), \dots, f_M(P)],$$

where $f_0, \dots, f_M \in K[X_0, \dots, X_N]$ are homogeneous polynomials of degree d with no common factors. The rational map φ is *defined at P* if at least one of the values $f_0(P), \dots, f_M(P)$ is non-zero. The rational map φ is called a *morphism* if it is defined at every point of $\mathbb{P}^N(K)$. If the polynomials $f_0, \dots, f_N$ have coefficients in a subfield L of K, we say that φ is *defined over L*.

For our purposes, we will often consider projective spaces over the field $\bar{\mathbb{Q}}$ of algebraic numbers (roots of polynomial equations over $\mathbb{Q}$), which will be covered in Lecture 2 if you are not already familiar with it. We will be able to define a very useful notion of height for points in such spaces, but for now we define the height in the simple case of *$\mathbb{Q}$-rational points* in $\mathbb{P}^N$ i.e. the set

$$\mathbb{P}^N(\mathbb{Q}) = \{[x_0, \dots, x_N] \in \mathbb{P}^N : \text{ all } x_i \in \mathbb{Q}\}.$$

Definition 4. Given a point $P = [x_0, \dots, x_N] \in \mathbb{P}^N(\mathbb{Q})$, we may assume that the homogeneous coordinates satisfy

$$x_0, \dots, x_N \in \mathbb{Z} \quad \text{and} \quad \gcd(x_0, \dots, x_N) = 1 \tag{1}$$

(see Question 2). Having done this, we define the *height* of P to be

$$H(P) = \max\{|x_0|, \dots, |x_N|\},$$

and the *logarithmic height* of P to be $h(P) = \log H(P)$.

Definition 5. Let $f \in \bar{\mathbb{Q}}[X_0, \dots, X_N]$ be a homogeneous polynomial. Then, we can define the *projective subvariety*

$$V(F) := \{P \in \mathbb{P}^n : f(P) = 0\}$$

cut out by F (see Question 3). We sometimes write $C : F = G$ as shorthand to denote $C = V(F - G)$, e.g. $E : Y^2 Z = X^3 - 432Z^3$ would mean $E := V(Y^2 Z - (X^3 + 432Z^3))$.

Earlier, we defined rational maps and morphisms between projective spaces. One can similarly define rational maps and morphisms between projective varieties. The general definition is a bit involved, but for the purposes of this problem set, examples of the following form suffice.

Definition 6. Let $f(X_0,\dots,X_N), g(X_0,\dots,X_M)$ be homogeneous polynomials cutting out projective subvarieties $X = V(f) \subset \mathbb{P}^N$ and $Y = V(g) \subset \mathbb{P}^M$. Let $\varphi_0,\dots,\varphi_M \in \bar{\mathbb{Q}}[T_0,\dots,T_N]$ be homogeneous polynomials all of the same degree d, so they define a rational map

$$\varphi := (\varphi_0,\dots,\varphi_M) : \mathbb{P}^N \dashrightarrow \mathbb{P}^M.$$

If $\varphi(P) \in Y(\bar{\mathbb{Q}})$ for all $P \in X(\bar{\mathbb{Q}})$ at which φ is defined, then the restriction $\varphi|_X : X \dashrightarrow Y$ gives an example of a *rational function from X to Y*. This φ will be a *morphism from X to Y* if $\varphi(P)$ is defined for all $P \in X(\bar{\mathbb{Q}})$ (even if $\varphi(P)$ is not defined for all $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$). If there exists a morphism $\psi : Y \to X$ so that $\varphi \circ \psi = \mathrm{id}_Y$ and $\psi \circ \varphi = \mathrm{id}_X$, then we say that φ (and so also ψ) is an *isomorphism.*

In general, one can define rational functions $X \dashrightarrow Y$ which do not necessarily extend to rational functions $\mathbb{P}^N \dashrightarrow \mathbb{P}^M$, but we will not see those in this problem set.

Example. Consider the elliptic curve $E : y^2 = x^3 - x$. There is an isomorphism $\varphi : E \to E$ given by $\varphi(x, y) = (-x, iy)$.

Beginner problems

Question 1. Let $x_1,\dots,x_n \in \mathbb{Q}$. Prove the following basic properties of the height $H(p/q) = \max\{|p|, |q|\}$ for rational numbers:

(a) $H(x_1 \cdots x_n) \leqslant H(x_1)\cdots H(x_n)$;
(b) $H(x_1 + \cdots + x_n) \leqslant nH(x_1)\cdots H(x_n)$.

Question 2. Show that given any point $P = [x_0,\dots,x_N] \in \mathbb{P}^N(\mathbb{Q})$, we may choose the homogeneous coordinates x_i to satisfy the conditions in (1).

Question 3. Let $f(T_0, T_1,\dots,T_n)$ be a homogeneous polynomial. Given a point $P = [x_0,\dots,x_n] \in \mathbb{P}^n(\bar{\mathbb{Q}})$, note that the expression $f(P) = f(x_0,\dots,x_n)$ is not well-defined; that is, its value can depend on a choice of representative for P. Despite this, show that the if $f(x_0,\dots,x_n) = 0$, then $f(y_0,\dots,y_n) = 0$ for any other choice of $y_0,\dots,y_n \in \bar{\mathbb{Q}}$ so that $P = [y_0,\dots,y_n]$. Because of this, our notation

$$V(f) := \{P \in \mathbb{P}^n : f(P) = 0\} \subset \mathbb{P}^n,$$

from Definition 1 is justified.

Question 4. Say $\mathbb{P}^2$ is given homogeneous coordinates $[X : Y : Z]$. Consider the elliptic curves

$$V := V(X^3 + Y^3 = Z^3) \text{ and } W := V(Y^2Z = X^3 - 432Z^3).$$

Show that $\varphi = [12Z, 36(X - Y), X + Y] : V \to W$ is a morphism. For something a bit harder, show that φ is in fact an isomorphism.

Question 5. Verify that $(1, 1)$ is a point of order 4 on the elliptic curve E_1: $y^2 = x^3 - x^2 + x$, and that $(0, 2)$ is a point of order 3 on the elliptic curve E_2: $y^2 = x^3 + 4$.

Question 6. We saw in lecture that the set

$$\left\{(a, b, c) \in \mathbb{Z}^3 : \gcd(a, b, c) = 1, a^2 + b^2 = c^2, \text{ and } z \neq 0\right\}$$

of primitive Pythagorean triples is in bijection with the set

$$P := \left\{(u, v) \in \mathbb{Q}^2 : u^2 + v^2 = 1\right\}$$

of rational points on the unit circle. We further saw that there is a map

$$\begin{array}{rccc} f: & \mathbb{Q} & \longrightarrow & P \\ & t & \longmapsto & \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \end{array}$$

which is injective with image $P\backslash\{(-1, 0)\}$. We want to give a projective interpretation of these observations.

(a) Convince yourself that we can view $\mathbb{Q}$ as a subset of $\mathbb{P}^1(\mathbb{Q})$ via $t \mapsto [t, 1]$. Similarly, show that we can view P as a subset of $\mathbb{P}^2(\mathbb{Q})$ via $(u, v) \mapsto [u, v, 1]$ and show that this in fact gives a bijection $P \cong C(\mathbb{Q})$ onto the $\mathbb{Q}$-points of $C := V(X^2 + Y^2 = Z^2)$.

(b) Show that the map $f : \mathbb{Q} \to P$ extends[1] to the rational map $\varphi : \mathbb{P}^1 \to C$ given by

$$\varphi([X, Y]) = [Y^2 - X^2, 2XY, Y^2 + X^2].$$

Furthermore, show that φ is in fact an isomorphism. Hence, primitive Pythagorean triples are parameterized by $\mathbb{P}^1(\mathbb{Q})$ without caveats (the missing point $(-1, 0) \in P$ from before now corresponds to the point $\infty := [1, 0] \in \mathbb{P}^1(\mathbb{Q})$).

Question 7. Show that the rational map $\varphi : \mathbb{P}^2 \to \mathbb{P}^2$ given by

$$\varphi([X, Y, Z]) = [X^2 - Y^2, XY - Z^2, Y^2 - Z^2]$$

is not a morphism.

Intermediate problems

Question 8. Verify that the doubling map for the elliptic curve $y^2 = x^3 + 1$ is given by

$$P = (x, y) \mapsto 2P = \left(\frac{x^4 - 8x}{4x^3 + 4}, \frac{2x^6 + 40x^3}{8y^3}\right).$$

Note that we cannot plug in the point $(-1, 0)$ on the curve into the formula above – can you explain why?

The map $f(x) = \frac{x^4 - 8x}{4x^3 + 4}$ is an example of a *Lattès map*. A Lattès map is a rational function (i.e. a ratio of two polynomials) that describes the x-coordinate of the point $2P$ in terms of the x-coordinate of P for some elliptic curve.

Question 9. Let

$$\nu(B) = \#\{P \in \mathbb{P}^N(\mathbb{Q}) : H(P) \leqslant B\}. \tag{2}$$

Find positive constants c_1 and c_2 such that

$$c_1 B^{N+1} \leqslant \nu(B) \leqslant c_2 B^{N+1}$$

for all $B \geqslant 1$.

Question 10. Consider the hyperplane

$$X := V(a_0 x_0 + \ldots + a_{N+1} x_{N+1}) \subset \mathbb{P}^{N+1}$$

where $a_0, \ldots, a_{N+1} \in \mathbb{Q}$ are not all zero. Show that, for each integer $M \geqslant 1$,

$$\{P \in X(\mathbb{Q}) : H(P) \leqslant M\} \leqslant C(2M + 1)^{(N+1)}$$

for some constant $C > 0$. [Hint: Construct an isomorphism between X and $\mathbb{P}^N$].

Question 11. Let $\varphi : \mathbb{P}^N \to \mathbb{P}^M$ be a rational map of degree d, defined over $\mathbb{Q}$. Prove that there exists a constant $C > 0$, depending only on φ, such that

$$h(\varphi(P)) \leqslant dh(P) + C$$

for all $P \in \mathbb{P}^N(\mathbb{Q})$ at which φ is defined.

In fact, if φ is a morphism, it is also possible to prove a lower bound of the form $h(\varphi(P)) \geqslant dh(P) - C$, but we will not yet do so. For now, consider the following example. View the map φ from Question 6 (b) as a morphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^2$ of degree 2, and compute explicit constants $C_1, C_2 > 0$ such that

$$2h(P) - C_1 \leqslant h(\varphi(P)) \leqslant 2h(P) + C_2$$

[1] By 'φ extends f' we mean that if $t \in \mathbb{Q}$, and $f(t) = (u, v)$, then $\varphi([t, 1]) = [u, v, 1]$.

for all $P \in \mathbb{P}^1(\mathbb{Q})$.

Question 12. For $P = [x_0, \dots, x_N] \in \mathbb{P}^N$ and $Q = [y_0, \dots, y_M] \in \mathbb{P}^M$, define

$$P \star Q = [x_0y_0, x_0y_1, \dots, x_iy_j, \dots, x_Ny_M] \in \mathbb{P}^{MN+M+N}.$$

The map $(P, Q) \mapsto P \star Q$ is called the *Segre embedding* of $\mathbb{P}^N \times \mathbb{P}^M$ into $\mathbb{P}^{MN+M+N}$.
Prove that

$$H(P \star Q) = H(P)H(Q)$$

for any $P \in \mathbb{P}^N(\mathbb{Q})$ and $Q \in \mathbb{P}^M(\mathbb{Q})$.

Question 13. Let $M = \binom{N+d}{N} - 1$ and let $f_0, \dots, f_M$ be the distinct monomials of degree d in the $N+1$ variables $X_0, \dots, X_N$. For any point $P = [x_0, \dots, x_N] \in \mathbb{P}^N$, let

$$P^{(d)} = [f_0(P), \dots, f_M(P)] \in \mathbb{P}^M.$$

The map $P \mapsto P^{(d)}$ is called the *d-uple embedding* of $\mathbb{P}^N$ into $\mathbb{P}^M$.
Prove that

$$H\left(P^{(d)}\right) = H(P)^d = H\left([x_0^d, \dots, x_N^d]\right)$$

for all $P = [x_0, \dots, x_N] \in \mathbb{P}^N(\mathbb{Q})$.

Question 14. This question deals with complex multiplication (CM) in elliptic curves, which will come up later in the course! Let E be an elliptic curve over $\mathbb{C}$.

(a) Show that $\mathbb{Z} \subseteq \mathrm{End}(E)$, where $\mathrm{End}(E)$ denotes the ring of morphisms $E \to E$ that are also group homomorphisms.
(b) We say that E has *complex multiplication* if $\mathbb{Z} \subsetneq \mathrm{End}(E)$. This is, E possesses "additional symmetries". Show that the curve $E : y^2 = x^3 - x$ has complex multiplication over $\mathbb{C}$.
(c) Find a curve E without complex multiplication. *Hint:* use the LMFDB!

Advanced problems

Question 15. When $N = 1$, prove that

$$\lim_{B \to \infty} \frac{\nu(B)}{B^2} = \frac{12}{\pi^2}.$$

where ν is defined as in (2) More generally, prove that the limit $C(N) := \lim_{B \to \infty} \nu(B)/B^{N+1}$ exists, and express it in terms of a value of the Riemann ζ-function. Can you prove the more precise asymptotic behaviour

$$\nu(B) = \begin{cases} \frac{12}{\pi^2}B^2 + O(B \log B) & N = 1, \\ C(N)B^{N+1} + O(B^N) & N > 1, \end{cases}$$

as $B \to \infty$?

Question 16. Let $E : y^2 = x^3 + Ax + B$ and $E' : y^2 = x^3 + A'x + B'$ be two elliptic curves. We let the same letters E, E' denote also the corresponding projective varieties

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3 \text{ and } E' : Y^2Z = X^3 + A'XZ^2 + B'Z^3.$$

Let $\varphi : E \to E'$ be an isomorphism such that $\varphi([0 : 1 : 0]) = [0 : 1 : 0]$. Show that φ must be of the form

$$\varphi([X, Y, Z]) = [\lambda^2 X : \lambda^3 Y : Z]$$

for some $\lambda \in \bar{\mathbb{Q}}$. Given that φ is of this form, write A', B' in terms of A, B, λ.