Math 223b: Algebraic Number Theory

Spring 2021

Problem set #6

due Monday, March 22 at noon

We assume that K is a number field throughout this problem set.

Problem 1. Let E be an elliptic curve over K and let $P, Q \in E(K)$. Show that $h_{[Q]}(P) \approx_Q h_{[O]}(P - Q)$ (where the difference bound depends only on E and Q, but not on P).

Problem 2. a) Show that for any $T \in \mathbb{R}$, there are only finitely many points $P \in \mathbb{P}^n(K)$ with $H(P) \leqslant T$.

b) Let $N(T)$ be the number of points $P \in \mathbb{P}^n(\mathbb{Q})$ with $H(P) \leqslant T$. Show that $N(T) \asymp T^2$ for $T \to \infty$.

c) (bonus) Let $N(T)$ be the number of points $P \in \mathbb{P}^n(K)$ with $H_K(P) \leqslant T$. Show that $N(T) \asymp_K T^{(n+1)[K:\mathbb{Q}]}$ for $T \to \infty$.

Problem 3. Let C be any smooth projective curve over $\mathbb{Q}$ of genus 0 with $C(\mathbb{Q}) \neq \varnothing$. Let $\varphi : C \to \mathbb{P}^n_{\mathbb{Q}}$ be a closed embedding. Show that there is an integer $m \geqslant 1$ such that $\#\{P \in C(\mathbb{Q}) \mid H(\varphi(P)) \leqslant T\} \asymp T^{2/m}$ for $T \to \infty$.

Problem 4. Consider a matrix $M \in \mathrm{GL}_{n+1}(K)$. It induces an automorphism φ of $\mathbb{P}^n_K$. Show that $h_K(\varphi(P)) \asymp_M h_K(P)$ for all $P \in \mathbb{P}^n_K(\overline{K})$.

Problem 5. a) Prove Corollary A.2.9: Let $f_0, \ldots, f_m \in K[X_0, \ldots, X_n]$ be homogeneous degree d polynomials, $A = \mathbb{P}^n_K \backslash V(f_0, \ldots, f_m)$ the set of points where $f_0, \ldots, f_m$ don't all vanish, and let $\varphi : A \to \mathbb{P}^m_K$ be the morphism defined by $f_0, \ldots, f_m$. Then $h(\varphi(P)) \lesssim_{f_0,\ldots,f_m} d \cdot h(P)$ for all $P \in A(\overline{K})$.

b) Prove Corollary A.2.10: Let $f_0, \ldots, f_m \in K[X_0, \ldots, X_n]$ be homogeneous degree d polynomials, $W \subseteq \mathbb{P}^n_K$ a variety with $W \cap V(f_0, \ldots, f_m) = \varnothing$, and let $\varphi : W \to \mathbb{P}^m_K$ be the morphism defined by $f_0, \ldots, f_m$. Then $h(\varphi(P)) \approx_{f_0,\ldots,f_m} d \cdot h(P)$ for all $P \in W(\overline{K})$.

Problem 6 (bonus)**.** Let $f, g \in \mathbb{Z}[X, Y]$ be nonzero homogeneous polynomials of degree d and assume that every coefficient c of f or g satisfies

$|c| \leqslant R$. Assume that f and g have no common zero in $\mathbb{P}^1(\overline{\mathbb{Q}})$. Show that for all $x, y \in \mathbb{Z}$ with $\gcd(x, y) = 1$, we have $\gcd(f(x, y), g(x, y)) \leqslant (2d)! \cdot R^{2d}$. (Hint: Resultant.)