

HOMEWORK ASSIGNMENT # 1

Due Tuesday, February 18

1. a. Let E be the elliptic curve given by $y^2 = x^3 + 17$, and let P be the point $(2, -5)$. Find the coordinates of the point $2P$.
 b. Find the coordinates (as complex numbers) of all 2-torsion and 3-torsion points on the elliptic curve E given by $y^2 = x^3 + 1$. (**Hint:** $3P = 0$ iff $2P = -P$).
2. a. Compute the absolute logarithmic heights $h(2+\sqrt{5})$ and $h(1/\sqrt[3]{7})$.
 b. Compute $|\frac{5+\sqrt{5}}{3}|_v$ and $\|\frac{5+\sqrt{5}}{3}\|_v$ for all places v of $\mathbf{Q}(\sqrt{5})$.
 c. Compute $h(1 : 2 : \frac{5+\sqrt{5}}{3})$.
3. Suppose L/K is a finite extension of number fields.
 - a. If $w \in M_L^0$ lies over $v \in M_K^0$, show that the restriction of the standard absolute value $|\cdot|_w$ to K is just $|\cdot|_v$. (You can take $w|v$ to mean that w corresponds to \mathfrak{q} , v corresponds to \mathfrak{p} , and $\mathfrak{q}|\mathfrak{p}$.) Prove an analogue of this for infinite places as well.
 - b. Show that if $K = \mathbf{Q}$ and $\beta \in L$, then for a fixed place $v \in M_{\mathbf{Q}}$,

$$\prod_{w|v} \|\beta\|_w = \|N\beta\|_v.$$

(Extra credit: Can you prove an analogue of this formula if K is a general number field?)

4. a. If ζ is a root of unity and $\alpha \in \overline{\mathbf{Q}}$, show that $h(\zeta\alpha) = h(\alpha)$.
 b. Describe explicitly the set of $\alpha \in \mathbf{P}^n(\overline{\mathbf{Q}})$ such that $h(\alpha) = 0$.
5. Suppose $\alpha \in \overline{\mathbf{Q}}^*$ is not a root of unity.
 - a. If $\deg(\alpha) = 2$, prove that $h(\alpha) \geq \frac{1}{2} \log \frac{1+\sqrt{5}}{2}$.
 - b. If $\deg(\alpha) = 3$, prove that $h(\alpha) \geq \frac{1}{3} \log \theta_0$ where θ_0 is the unique real root of $x^3 - x - 1$. [If you need to use a computer, include the source code in your solution.]
6. (Extra credit) The goal of this exercise is to prove that if $\alpha \in \overline{\mathbf{Q}}^*$ has degree d and α is not a root of unity, then $h(\alpha) > \frac{1}{11d^3}$. [Lehmer's conjecture predicts that in fact $h(\alpha) > \frac{c}{d}$ for some absolute constant $c > 0$. It is known, following work of Dobrowolski and Voutier, among others, that for $d \geq 2$ we have $h(\alpha) > \frac{1}{4d} \left(\frac{\log \log d}{\log d} \right)^3$.] It is clearly enough to assume that α is an algebraic integer with a fixed embedding into \mathbf{C} . Let $\bar{\alpha}$ (the "house" of α) denote the

maximum complex modulus of the conjugates $\alpha_1, \dots, \alpha_d$ of α , and for all positive integers n , let $S_n := \sum_{j=1}^d \alpha_j^n$.

a. Show that $S_n \in \mathbf{Z}$ for all n , and that

$$S_n \equiv S_n^p \equiv S_{np} \pmod{p}.$$

b. Let p be a prime with $2ed < p < 4ed$, which exists by “Bertrand’s postulate”. Use the inequality $|S_n| \leq d\bar{\alpha}^n$ to show that if

$$\bar{\alpha} \leq 1 + \frac{1}{4ed^2},$$

then $|S_n - S_{np}| \leq 2de < p$ for $1 \leq n \leq d$.

c. Using the fact that α is not a root of unity, show that

$$\bar{\alpha} > 1 + \frac{1}{4ed^2}.$$

d. Now use the inequality

$$\left(1 + \frac{1}{4ed^2}\right)^{11d^2} > e$$

for $d \geq 2$ to prove that $h(\alpha) > \frac{1}{11d^3}$.