# Math 223b: Algebraic Number Theory

## Spring 2021

### Problem set #5

due Monday, March 15 at noon

We assume that the field $K$ has characteristic 0 throughout this problem set.

**Problem 1.** Let $C$ be a smooth projective curve over $K$. Show that if there is a nonconstant morphism $\phi : \mathbb{P}^1_K \to C$ defined over $K$, then $C \cong \mathbb{P}^1_K$ over $K$.

**Problem 2.** Let $G$ be an abelian group such that for all $m \geqslant 1$, the group $G[m]$ of $m$-torsion points has size $m^2$. Show that $G[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$.

**Problem 3.** Consider an elliptic curve $E$ given by the equation $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$. Let $\psi : E \to \mathbb{P}^1$ be the morphism sending $[x : y : z] \neq O$ to $[x : z]$. Show that for every $m \geqslant 1$, there is a (unique) morphism $F_m : \mathbb{P}^1 \to \mathbb{P}^1$ such that $\psi \circ [m] = F_m \circ \psi$.

**Problem 4** (Use a computer!)**.** Consider the elliptic curve $E$ given by the equation $Y^2Z = X^3 + 11Z^3$ and the (non-torsion) point $P = [-14 : 19 : 8]$ on $E(\mathbb{Q})$. Let $\psi : E \to \mathbb{P}^1$ be the map sending $[x : y : z]$ to $[x : z]$. Define the height $H(Q) \in \mathbb{Z}$ of a point $Q \in \mathbb{P}^n(\mathbb{Q})$ as in the second lecture. For $m = 1, \ldots, 20$, compute $\log(H(m \cdot P))/m^2$ and $\log(H(\psi(m \cdot P)))/m^2$ (up to at least four decimal places).

**Problem 5** (not graded, skip if you've done this before)**.** Consider an elliptic curve $E$ given by the equation $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$.

Let $P = [x : y : z] \in E$ with $P \neq [0 : 1 : 0]$

a) If $y \neq 0$, show that the point $2P = [x' : y' : z']$ satisfies

$$[x' : z'] = [x^4 - 2a_4x^2z^2 - 8a_6xz^3 + a_4^2z^4 : 4(x^3 + a_4xz^2 + a_6z^3)z].$$

b) Show that $P$ is a three-torsion point if and only if

$$3x^4 + 6a_4x^2 + 12a_6x - a_4^2 = 0.$$

**Problem 6** (bonus)**.** Assume that $K$ is algebraically closed. Let $C$ be a smooth projective curve and assume that there is a divisor $D$ on $C$ with $0 < \deg(D) < 2g_C - 2$ and $l(D) = \frac{1}{2}\deg(D) + 1$.

a) Show that there is a divisor $D'$ with $\deg(D) = 2$ and $l(D) = 2$. (Hint: Look at our proof that $l(D) \leqslant \frac{1}{2}\deg(D) + 1$. Use downward induction.)

b) Show that there is a degree two morphism $C \to \mathbb{P}^1$.