18.704 Fall 2004 Homework 5

All references are to the textbook "Rational Points on Elliptic Curves" by Silverman and Tate, Springer Verlag, 1992. Problems marked **(*)** are more challenging exercises that are optional but not required.

1. This problem is meant to show that the height function can have subtle properties, even though its definition is very simple.

For any integer $\kappa \geq 1$, define

$$R(\kappa) = \{q \in \mathbb{Q} \,|H(q) \leq \kappa\}.$$

Notice that any $q \in R(\kappa)$ has the form $q = m/n$ where $0 \leq |m| \leq \kappa$ and $0 \leq |n| \leq \kappa$. Let $\#R(\kappa)$ be the number of elements in $R(\kappa)$. Then we trivially get the bound $\#R(\kappa) \leq (2\kappa + 1)^2$ for all κ, because there are $2\kappa + 1$ integers m satisfying $0 \leq |m| \leq \kappa$, and similarly for $|n|$. Of course this is a severe overcounting, since different choices of m, n can lead to the same rational number q.

(a) Give a better bound for $\#R(\kappa)$. More specifically, give a bound of the following form:

$$\#R(\kappa) \leq \alpha\kappa^2 + \beta\kappa + \gamma \text{ for all } \kappa \geq 1,$$

Where α, β, γ are some constants, and with $\alpha \leq 3/2$.

(b) Explain how you would go about finding better and better bounds for $\#R(\kappa)$ (i.e. with a smaller values of α). You don't have to calculate these bounds exactly; I just want you to describe a some kind of algorithm you could use to find them.

(c) (*) There is a limit to this process: Can you prove Exercise 3.1(b) of the text? (I'm not sure how to do it.)

2. Let P be a rational point on the nonsingular curve C in Weierstrass form. This exercise concerns a question one of you had in class: if P has infinite order, is it possible for all of the points $P, 2P, 3P, \ldots$ to have integer coefficients? You will answer this question in part (c) below.

(a) Suppose that there is a number $N > 0$ such that $H(mP) \leq N$ for infinitely many $m \geq 1$. Prove that the point P has finite order in the group of rational points.

(b) Write $mP = (x_m, y_m)$ for all $m \geq 1$. Show that there is a constant $N > 0$ such that $|x_m| \leq N$ for infinitely many $m \geq 1$. (Suggestion: Consider the sequence of points $P, 2P, 4P, 8P, \ldots$ and use the formulas for doubling a point. Show that given any point Q, if the x coordinate of Q is very large then the x-coordinate of $2Q$ must be much smaller in absolute value.)

(c) Suppose now that mP has integer coordinates for all $m \geq 1$, in other words $x_m, y_m \in \mathbb{Z}$ for all $m \geq 1$. Show that the point P has finite order in the group of rational points. (Even if you don't succeed in proving part (b), feel free to assume part (b) is true in your proof of this part.)