18.704 Fall 2004 Homework 10

Due 12/03/04

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. Let $\beta > 0$ be an irrational real number.

(a) For each integer $n \geq 0$, define $\delta(n) = n\beta - [n\beta]$, where $[c]$ means the greatest integer less than or equal to c. Show that the set of real numbers $\{\delta(n) | n \in \mathbb{Z}, n \geq 0\}$ is dense in the real interval $(0, 1)$. In other words, given any real number $0 < a < 1$ and $\epsilon > 0$, show that there exists some n such that $|a - \delta(n)| < \epsilon$.

(b) Using part (a), show that given any constant $C > 0$, there exist infinitely many distinct rational numbers p/q such that

$$\left| \frac{p}{q} - \beta \right| \leq \frac{C}{q}.$$

2. Let $\beta \in \mathbb{R}$ be any real number. In this exercise we will consider solutions to the inequality

$$\left| \frac{p}{q} - \beta \right| \leq \frac{1}{q^3}. \tag{0.1}$$

We will eventually prove in Section V of the book that there are finitely many rational numbers p/q satisfying (0.1), at least when β is the irrational cube root of an integer. The point of this exercise is to show that in any case, in any list of solutions to an equation (0.1) the denominators must grow very rapidly, so the solutions are quite sparse.

Now do Exercise 5.8 parts (a) and (b) from the text.

3. For this exercise, we will look at the curves $C_d : y^2 = x^3 + d$, where $d \in \mathbb{Z}$. Let $C_d(\mathbb{Z})$ denote the set of integer points on the curve.

(a) Show that for some choice of $d \geq 1$ the group $C_d(\mathbb{Q})$ contains a point of infinite order (i.e. has rank ≥ 1.)

(b) Do Exercise 5.6(b) from the text. This proves that curves of the form C_d can contain arbitrarily large numbers of integer points.