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

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

Solution. (a) Set $S = \{\delta(n) | n \geq 0\}$ and note that $S \subset [0, 1]$. Since $[0, 1]$ is compact, we can find a subsequence $n_1 < n_2 < n_3 < \dots$ of $1, 2, 3, \dots$ such that the sequence $\delta(n_i)$ converges as $i \to \infty$ to some point $d \in [0, 1]$. In particular, given $1 > \epsilon > 0$ we can certainly find integers $r > s > 0$ such that $|\delta(s) - d| \leq \epsilon/2$ and $|\delta(r) - d| \leq \epsilon/2$; then

$$|\delta(r) - \delta(s)| \leq |\delta(s) - d| + |\delta(r) - d| < \epsilon.$$

We claim that $|\delta(r) - \delta(s)| = \delta(r - s)$. This is because $|\delta(r) - \delta(s)|$ and $\delta(r - s)$ are both in the interval $(0, 1)$ (since β is irrational) and

$$|\delta(r) - \delta(s)| - \delta(r - s) \in \mathbb{Z}.$$

Setting $p = r - s$, we have $\delta(p) < \epsilon$. Let m be the largest integer such that $mp < 1$. Then by a similar argument as above, we have $\delta(ip) = i\delta(p)$ for all $1 \leq i \leq m$. So the sequence of points

$$\delta(p), \delta(2p) = 2\delta(p), \dots, \delta(mp) = m\delta(p)$$

gives a sequence of points in S such that every point in $[0,1]$ lies at a distance of at most $\delta(p) < \epsilon$ from one of them. Since ϵ was arbitrary, it follows that S is dense in $[0,1]$.

(b) By part (a), for each integer $n > 0$ we can find $r_n > 0$ such that $0 < \delta(r_n) < 1/n$. Then putting $q_n = r_n$ and $p_n = [r_n\beta]$, we have $|p_n - q_n\beta| < 1/n$. Then dividing by q_n, we get

$$\left|\frac{p_n}{q_n} - \beta\right| < \frac{1}{nq_n}.$$

In particular, we get a sequence of rational numbers p_n/q_n, and given any $C > 0$ it is clear that

$$\left|\frac{p_n}{q_n} - \beta\right| < \frac{C}{q_n}$$

will hold for all n sufficiently large, in particular for infinitely many n. Also, there are infinitely many distinct rational numbers among the p_n/q_n, since the differences $\left|\frac{p_n}{q_n} - \beta\right|$ go to zero as n increases.

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.

Solution. (a) Consider distinct rationals p/q and p'/q' such that $q' > q$ and satisfying

$$\left|\frac{p}{q} - \beta\right| \leq \frac{1}{q^3} \text{ and} \left|\frac{p'}{q'} - \beta\right| \leq \frac{1}{(q')^3}.$$

Then by the triangle inequality, we see that

$$\left|\frac{p}{q} - \frac{p'}{q'}\right| \leq \frac{1}{q^3} + \frac{1}{(q')^3} \leq \frac{2}{q^3}.$$

Multiplying by qq', we have

$$|pq' - qp'| \leq \frac{2q'}{q^2}.$$

Now since we assume that p/q and p'/q' are distinct rationals, we have that $pq' - qp'$ is a nonzero integer, so $|pq' - qp'| \geq 1$. So $\dfrac{2q'}{q^2} \geq 1$ and thus $q' \geq \dfrac{q^2}{2}$ as required.

(b) Now if $p_0/q_0, \ldots p_r/q_r$ all satisfy the inequality, with $4 \leq q_0 \leq q_1 \leq \cdots \leq q_r$, then the trick is to prove that actually $q_r \geq 2^{2^r+1}$, which is an even better estimate than the estimate $q_r \geq 2^{2^r}$ which we want, but is more natural to prove by induction.

The base case is $q_0 \geq 4 = 2^2$. For the induction step, we assume the estimate holds for r and then using part (a) we get

$$q_{r+1} \geq \frac{q_r^2}{2} \geq 2^{2^{r+1}+2}/2 = 2^{2^{r+1}+1}.$$

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.

Solution. (a). It is not hard to cook up an example by picking some small d. For example, taking $d = 3$, we have the point $P = (1, 2)$ on $C : y^2 = x^3 + 3$. One calculates that $2P = (-23/16, -11/64)$. Since this point does not have integer coefficients, the point P has infinite order by the Nagell-Lutz Theorem.

(b). Take some integer point P of infinite order on $C : y^2 = x^3 + d$ for some d (by part (a) we know that some such exists). Then consider the points $2^n P = (p_n/q_n, r_n/s_n)$ for $n \geq 0$, where the p_n/q_n and r_n/s_n are rational numbers written in lowest terms. Note that if (x_0, y_0) is a point in $C(\mathbb{Q})$, then if $e \in \mathbb{Z}$ clears the denominators of x_0 and y_0, i.e. $ex_0, ey_0 \in \mathbb{Z}$, then $(e^2 x_0, e^3 y_0)$ is an integer point on $C' : y^2 = x^3 + e^6 d$.

So considering the first $n+1$ points in the sequence $P, 2P, 4P, \ldots$, we have that $e_n = \operatorname{lcm}(q_1, q_2, \ldots, q_n, s_1, \ldots, s_n)$ clears all of the denominators of these points. Then we have at least $n+1$ integer points on the curve $y^2 = x^3 + e_n^6 d$, namely the points

$$\left\{ \left(\frac{e_n^2 p_i}{q_i}, \frac{e_n^3 r_i}{s_i} \right) \middle| 0 \leq i \leq n \right\}.$$

To estimate the size of the constant $e_n^6 d$, we use a lemma from Chapter III of the text (recall the height notation from that chapter.) In particular we know that there is a constant $\kappa > 0$ such that $h(2P) \leq 4h(P) + \kappa$. By induction one can use this to get the estimate $h(2^i P) \leq 4^i (h(P) + \kappa)$ for all $i \geq 0$.

In fact, we know from earlier results that the same primes divide s_n as q_n, in fact that $q_n^2 = s_n^3$. So $q_n^2 \leq H(2^n P)$ by the definition of the height of a point (remember this is the height of the x-coordinate), and then $2 \log q_n = 3 \log s_n \leq h(2^n P)$ for each n.

Now

$$e_n = \text{lcm}(q_1, q_2, \ldots, q_n, s_1, \ldots, s_n) = \text{lcm}(q_1, \ldots, q_n) \leq q_1 q_2 \ldots q_n$$

and so

$$\log\ (e_n)^6 d = \log d + 6 \log e_n \leq N + \sum_{i=1}^{n} h(2^i P)/2$$

for some constant N. So

$$\log\ (e_n)^6 d \leq N + \sum_{i=1}^{n} 4^i M \leq N + 4^{n+1} M$$

for some constant M. Then $\log(\log(e_n)^6 d) \leq K + (n+1)L$ for constants K and L, and all n.

Finally, if we set $d_n = (e_n)^6 d$ for each n, then we see that the curve C_{d_n} has at least $n+1$ points by construction. Note that we can choose a constant $J > 0$ such that $(n+1) \geq J(K + (n+1)L)$ for all $n \geq 0$. So

$$\#C_{d_n}(\mathbb{Z}) \geq n + 1 \geq J \log \log d_n$$

for all $n \geq 0$, which proves the estimate we wanted.