18.704 Fall 2004 Homework 5 Solutions

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

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

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.)

Solution. (a) Consider the ordered integer pairs (m, n) with $|m| \leq \kappa$, $|n| \leq \kappa$. As we noted above, there are $(2\kappa + 1)^2$ of these. As (m, n) ranges over all such pairs, m/n ranges over the rational numbers q with $H(q) \leq \kappa$. But we are overcounting: First, there is no reason to ever take $n = 0$, and $m = 0$ need only be taken once. Also, we only need to take points in two out of the four quadrants, so we might as well assume that $n \geq 1$. This brings the number down: we have $2\kappa^2$ points (m, n) with $m \neq 0$, $n \geq 1$, and $H(m/n) \leq \kappa$, and we

also need one point with $m = 0$, say $(0, 1)$, bringing us down to $2\kappa^2 + 1$ possible ordered pairs.

Of course, we can do better, we should only count ordered pairs where m, n are relatively prime. But the number of these seems hard to count, so we go one prime at a time. Let us count the number of ordered pairs (m, n) where $m \neq 0$, $n \geq 1$, $H(m/n) \leq \kappa$, and both m, n are divisible by 2. This number is $2[\kappa/2]^2$, where $[r]$ means the largest integer less than or equal to r. Since $2[\kappa/2]^2 \geq 2((\kappa - 1)/2)^2$, when we throw away these bad ordered pairs, we are left with at most

$$\#R(\kappa) \leq 2\kappa^2 + 1 - (2/4)(\kappa - 1)^2 = (3/2)\kappa^2 + \beta\kappa + \gamma$$

which is the required bound.

(b) We can continue in the same way, throwing away next all of the ordered pairs where both coordinates are divisible by 3. But then we have to count carefully, because some of those ordered pairs also have both coordinates divisible by 2. In any case we get from this a bound of the form

$$\#R(\kappa) \leq 2\kappa^2 + 1 - 2[\kappa/2]^2 - 2[\kappa/3]^2 + 2[\kappa/6]^2$$

which gives a bound with smaller α. We could continue by next considering the prime 5, etcetera.

So the general algorithm is: consider the first m primes, $p_1, p_2, \ldots, p_m$. Then one can get an upper bound for $\#R(\kappa)$ by considering a sum of the form

$$1 + 2\kappa^2 - \sum_{1 \leq i \leq m} 2[\kappa/p_i]^2 + \sum_{1 \leq i < j \leq m} 2[\kappa/p_i p_j]^2 - \cdots + (-1)^m 2[\kappa/p_1 p_2 \cdots p_m]^2.$$

(A formula like this is derived by using the "principle of inclusion/exclusion." I'm happy if you just gave some idea of the process in words instead of writing a formula.)

(c) Most of you successfully solved this problem, which asks you to show that $\lim_{\kappa \to \infty} \#R(\kappa)/\kappa^2 = 12/\pi^2$. One way is to calculate the limit of the process described in part (b). Another is to express $\#R(\kappa)$ in terms of Euler's ϕ-function and use known results about this function. If you didn't get this part and want to know the solution, ask a classmate or come talk to me.

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.)

Solution. (a). If such a N exists, then there is a sequence of integers $m_1, m_2, \ldots$ such that $\{m_i P \mid i \geq 1\} \subset S(N)$ where

$$S(N) = \{(x, y) \in C(\mathbb{Q}) | H(x, y) \leq N\}.$$

As we saw in Section III.1, the set $S(N)$ is a finite set (this is more or less Lemma 1 of that section.) Since there are only finitely many possibilites for the points $m_i P$, this forces $m_i P = m_j P$ for some integers $m_i < m_j$. But then $(m_j - m_i)P = \mathcal{O}$, so P has finite order.

(b) On page 31 of the text a doubling formula for the x-coordinate is given. It shows that if $Q = (x, y) \in C(\mathbb{Q})$, then setting $2Q = (x', y')$ we have

$$x' = \frac{g(x)}{h(x)}$$

where $g(x) = x^4 + g'(x)$ and $h(x) = 4x^3 + h'(x)$. Here $g'(x)$ has degree 3 and $h'(x)$ has degree 2 but we will only care about the highest degree terms, since for large x, the lower degree terms are small by comparison. In fact, we can find $N > 0$ such that for all $|x| \geq N$ we have $|g'(x)| < |x|^4$ and $|h'(x)| < |x|^3$. Then for $|x| \geq N$ it follows that $|g(x)| \leq 2|x|^4$ and $|h(x)| \geq 3|x|^3$. Then if $|x| \geq N$, we have $|x'| \leq (2/3)|x|$.

It follows from this that given any point $Q = (x, y) \in C(\mathbb{Q})$, then if $|x| \geq N$, we have $2Q = (x', y')$ with $|x'| \leq (2/3)|x|$. Then we can find $n \geq 1$ such that $2^n Q = (x', y')$ with $|x'| \leq N$.

Now recall that we write $mP = (x_m, y_m)$. Starting with our given point P, we apply the above argument to show that there is some $n_1 \geq 1$ such that $2^{n_1} P$ has x-coordinate $\leq N$. Then we apply the argument to the point $2^{n_1} P$, to show there is some $n_2 > n_1$ such that $2^{n_2} P$ has x-coordinate $\leq n$. Continuing, we get an infinite sequence of numbers $n_1, n_2, \ldots$ such that $2^{n_i} P$ has x-coordinate of absolute value $\leq N$, for all $i \geq 1$.

(c) This is a combination of parts (a) and (b). If the points $mP = (x_m, y_m)$ all have integer coordinates, then this implies that $H(mP) = |x_m|$ for all $m \geq 1$. Then part (b) implies that there is a number N such that $H(mP) \leq N$ for infinitely many m. Part (a) now says that P has finite order.