18.704 Fall 2004 Homework 6 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. Do Exercise 3.4 of the text, which asks you to prove the upper bound in Lemma $3'$(b). Advice: use the proof of Lemma 2 in section III.2 as a model.)

Solution. This really is very similar to the endgame of the proof of Lemma 2, but easier. Let H and h be the height functions defined in section III.1. Let $\phi(x)$, $\psi(x)$ be two polynomials with no common roots, and let d be the maximum of the degrees of ϕ, ψ.

Let $q = m/n$ in lowest terms, so $H(q) = \max\{|m|, |n|\}$ by definition. Assume that $\psi(q) \neq 0$.

Write $\phi(x) = \sum_{i=0}^{d} a_i x^i$ and $\psi(x) = \sum_{i=0}^{d} b_i x^i$. Then we define

$$\Phi(q) = n^d \phi(q) = \sum_{i=0}^{d} a_i m^i n^{d-i}, \text{ and } \Psi(q) = n^d \psi(q) = \sum_{i=0}^{d} b_i m^i n^{d-i}$$

which are both integers. Now $\phi(q)/\psi(q) = \Phi(q)/\Psi(q)$. Although the fraction $\Phi(q)/\Psi(q)$ might not be in lowest terms, we still have

$$H\left(\frac{\phi(q)}{\psi(q)}\right) \leq \max\big(|\Phi(q)|, |\Psi(q)|\big)$$

and moreover,

$$|\Phi(q)| \leq \big(\sum_{i=0}^{d} |a_i||m|^i|n|^{d-i}\big) \leq \big(\sum_{i=0}^{d} |a_i|\big) H(q)^d.$$

Similarly,

$$|\Psi(q)| \leq \big(\sum_{i=0}^{d} |b_i|\big) H(q)^d.$$

So setting $A = \max\big(\sum_{i=1}^{d} |a_i|, \sum_{i=1}^{d} |b_i|\big)$, we have

$$H\left(\frac{\phi(q)}{\psi(q)}\right) \leq AH(q)^d$$

so taking logs we get

$$h\left(\frac{\phi(q)}{\psi(q)}\right) \leq dh(q) + \log A$$

and setting $\kappa_2 = \log A$ we've proven the bound requested.

2. The Nagell-Lutz theorem is not the last word when it comes to finding points of finite order on a nonsingular cubic curve C, but in special cases one can prove further necessary conditions. In this problem assume that C is a nonsingular cubic curve of the special form $y^2 = x^3 + ax^2 + bx$, with $a, b \in \mathbb{Z}$.

(a) As a warmup, prove the following fact: Let $\theta : G \to H$ be a homomorphism of commutative groups. If $g \in G$ has finite order, then $\theta(g) \in H$ has finite order.

(b) Now do Exercise 3.7(a) of the text.

Solution. (a) This part is really only here to give you a hint as to how to proceed in part (b). Anyway, the proof is trivial: g has finite order means that $mg = e$ for some $m \geq 1$, where e is the identity of G. Then $m\theta(g) = \theta(mg) = \theta(e) = e'$, where e' is the identity of H. This says that $\theta(g)$ has finite order in H.

(b) The key observation to make is that the homomorphism $\phi : C \to \overline{C}$ defined in section III.4 is helpful here. There $\overline{C}$ is defined to be the elliptic curve $y^2 = x^3 + \overline{a}x^2 + \overline{b}x$, where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$. The map ϕ is defined on coordinates as

$$\phi(x, y) = (y^2/x^2, y(x^2 - b)/x^2)$$

for all points $(x, y) \in C$ not equal to $\mathcal{O}$ or $T = (0, 0)$. We also note that $y^2/x^2 = x + a + (b/x)$ since (x, y) is a point on C.

Now let $P = (x, y) \in C(\mathbb{Q})$ have finite order. By the Nagell-Lutz theorem, x and y are integers. By part (a), $\phi(P)$ has finite order in $\overline{C}$. Since we assume $y \neq 0$, the formula above for ϕ works. Also, $\phi(P)$ must have integer coordinates, by the Nagell-Lutz theorem applied to $\overline{C}$. So $x + a + (b/x)$ is an integer. Since x and a are also integers, this implies that x divides b. Moreover, since $x + a + (b/x) = y^2/x^2$, we must also have that x divides y. Then the quantity $y^2/x^2 = (y/x)^2$ is a perfect square in $\mathbb{Z}$, i.e. $x + a + (b/x)$ is a perfect square.

3. With the help of the results of problem 2(b) above, in this problem we will generalize a problem from an earlier homework set.

(a) Find all possible primes p and integers $m \geq 0$ such that $p^m + 1$ is a perfect square.

(b) Let C be the curve $y^2 = x^3 + p^m x$ for some prime $p \geq 5$ and $m \geq 1$. Find all of the rational points of finite order on C (don't forget $\mathcal{O}$).

(c) It is not hard to find all of the rational points of finite order on $y^2 = x^3 + p^m x$ when $p = 2$ or $p = 3$, but the calculation is a bit tedious. So I'll ask you just to do a special case: find all of the rational points of finite order on $y^2 = x^3 + 64x$.

Solution.

(a). Suppose that $p^m + 1 = n^2$ for some integer $n \geq 1$, prime p, and $m \geq 0$. Then $p^m = n^2 - 1 = (n+1)(n-1)$. Suppose that $n-1 > 1$. Then also $n+1 > 1$, and so p divides both $n+1$ and $n-1$. but then p divides $(n+1)-(n-1) = 2$. So $p = 2$. furthermore, in this case, $n+1$ and $n-1$ are powers of 2 which differ by 2. This clearly forces $n-1 = 2$ and $n+1 = 4$, so $n = 3$ and $m = 3$.

Obviously $n - 1 = 0$ is forbidden, since p^m is positive, so we are left with the case $n - 1 = 1$. Then $n = 2$, $p = 3$, and $m = 1$.

So there are only two possibilities: $2^3 + 1 = 3^2$, and $3^1 + 1 = 2^2$.

(b) Fix the prime power p^m with $p \geq 5$ and $m \geq 1$. The rational points of order dividing 2 on $y^2 = x^3 + p^m x$ are precisely $\mathcal{O}$ and the points $(x, 0)$, where x is a rational root of $x^3 + p^m x$. Since $x^2 + p^m$ has complex roots, $\mathcal{O}$ and $(0, 0)$ are the only rational points of order dividing 2.

Now let $(x, y) \in C(\mathbb{Q})$ be a point of finite order bigger than 2. By problem $2(b)$ above, we know that $x | p^m$, and so $x = p^e$ is a prime power for some $0 \leq e \leq m$. Also, we know that $x + (p^m/x) = p^e + p^{m-e}$ is a perfect square.

Now we have several cases. Suppose that $e < m - e$. Then $p^e + p^{m-e} = p^e(1 + p^{m-2e})$ is a perfect square. Since p does not divide $1 + p^{m-2e}$, this means that e is even, and $(1 + p^{m-2e})$ is a perfect square. By part (a), this forces $p = 2$ or $p = 3$, contradicting the assumption $p \geq 5$ in this part.

Similarly, if $e > m - e$, we get a contradiction for essentially the same reason.

Finally, we have the case $e = m - e$, or $m = 2e$. Then $p^e + p^e = 2p^e$ must be a perfect square. Clearly for this to happen we need to have $p = 2$, which again is not allowed by the hypothesis.

We conclude that $\{\mathcal{O}, (0, 0)\}$ is the entire set of rational points of finite order on this C.

(c) In this part we assume that $p = 2$ and $m = 6$. We begin as in part (b): The rational points of order dividing two are $\{\mathcal{O}, (0, 0)\}$, so assume that (x, y) is a rational point of order > 2; then $x = 2^e$ for some $0 \leq e \leq 6$, and $2^e + 2^{6-e}$ is a perfect square.

Now because m is so small, we could just check all 7 possibilities for e, but let's continue to proceed as in part (b). So if $e < 6 - e$, then as above e is even and $1 + 2^{6-2e}$ is a perfect square. By part (a), $6 - 2e = 3$ and so there is no such e.

Similarly, if $e > 6 - e$ we get no solutions.

Finally, we have the case $e = 6 - e$, and so $e = 3$, and $2^3 + 2^3 = 16$ is indeed a perfect square in this case. So we get the candidate point $P = (8, 32)$ in this case. We need to check if it really does have finite order. We calculate the slope of the tangent line to P is $(3(8)^2+64)/2(32)=4$ and so $x(2P)=4^2-2(8)=0$. Then clearly $2P=(0,0)$.

So in this case, the group of rational points of finite order on C is

$$\{\mathcal{O},(0,0),P,-P\},$$

where $P=(8,32)$. The calculation above makes it clear that this is a cyclic group of order 4.