18.704 Fall 2004 Homework 6

On Homework #6 Problem 3 parts (b), (c), these parts should ask you to find all of the rational points of finite order.

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.)

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.

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 $y^2 = x^3 + 64x$.