# 18.704 Fall 2004 Homework 4

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.** In class we discovered an error in the textbook near the top of page 52. Recall the situation: we started with a curve in Weierstrass form in the $(x, y)$ plane, then changed coordinates to $(t, s)$ via $t = x/y$, $s = 1/y$, so the curve became

$$s = t^3 + at^2s + bts^2 + cs^3$$

with new additive identity point $\mathcal{O} = (0, 0)$ (the origin). Let $R$ be the set of all rational numbers with no $p$ in the denominator (when written in lowest terms), and for each $\nu \geq 1$ set

$$C(p^\nu) = \{(t, s) | t \in p^\nu R, s \in p^{3\nu} R\}.$$

Now if $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ are two different points on $C$ such that $t_1 = t_2$ and $P_1, P_2 \in C(p^\nu)$, prove that $P_1 + P_2 \in C(p^\nu)$. (The book claims that this is true because $P_1 = -P_2$, which is a false statement.)

**2.** Do Exercise 2.10 from the textbook.

**3.**(*****) Consider the curve

$$C : y^2 = x^3 + dx$$

where $d \in \mathbb{Z}$ is any integer.

(a) Exercise 3.7(c) on page 105 of the text gives a table showing what the group of rational points of finite order on $C$ is, for each possible $d$. Show that this table is incorrect.

(b) After some experimentation, make some conjecture about what the correct table should be.

(c) Can you prove your conjecture? (The result of Exercise 3.7(a) might be helpful.)