PROBLEM SET 7, DUE NOVEMBER 30TH

(1) Compare [Silverman-Tate problem IV 4.7]: Let $b \equiv 11(\bmod 15)$ and $c \equiv 4(\text{mod}15)$ be integers. Show that the cubic curve C corresponding to

$$y^2 = x^3 + bx + c$$

is smooth, and that $C(\mathbb{Q})$ contains no points of finite order except O.

(2) What is the maximal number of points $\#C(\mathbb{F}_{11})$ of a smooth cubic C corresponding to an equation $y^2 = x^3 + ax^2 + bx + c$ over $\mathbb{F}_{11}$? Give an example of such a cubic C and show that in your example $C(\mathbb{F}_{11})$ is a cyclic group.

(3) Let p be a prime number and suppose C corresponding to $y^2 = x^3 + ax^2 + bx + c$ is a smooth cubic over $\mathbb{F}_p$. Prove that if $\#C(\mathbb{F}_p) \equiv 1(\text{mod}p)$ and $p > 3$, then $\#C(\mathbb{F}_p) = p + 1$. Give an example showing that the same conclusion for $p = 3$ is incorrect.