18.704 Fall 2004 Homework 8

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. A nonsingular projective conic with at least one point over the field $\mathbb{F}_p$ has exactly $p+1$ projective points; the reason is that one can project onto a line as is argued on page 109 of the text. In this problem we see that the same is not true for singular conics. Let $p \neq 2$ be a prime, and let C be the conic given by the homogeneous equation $C : aX^2 + bXY + cY^2 = dZ^2$ where $a, b, c, d \in \mathbb{F}_p$ and $a, b, d \neq 0$. Let $\#C(\mathbb{F}_p)$ be the number of points on C in projective space over $\mathbb{F}_p$.

(a) Note that C is the given by the vanishing of $F(X, Y, Z) = aX^2 + bXY + cY^2 - dZ^2$ in $\mathbb{P}^2$. Recall that C is nonsingular at a point as long as not all partial derivatives of F vanish there. Show that C is nonsingular if and only if $b^2 = 4ac$.

(b) Assume that C is singular. Then do Exercise 4.1(b) from the text. For $p = 3$, find choices of a, b, c, d for which each possibility occurs.

2. (a) Let C be the projective curve $x^3 + y^3 + z^3 = 0$ which is the subject of Gauss's theorem. Calculate $\#C(\mathbb{F}_p)$ for $p = 307$ (you don't need a computer; see the suggestions on page 118.)

(b) Let p be a prime with $p \equiv 2 (\mathrm{mod}\, 3)$, and let $c \in \mathbb{F}_p$. Prove that the curve $C : y^2 = x^3 + c$ satisfies $\#C(\mathbb{F}_p) = p + 1$.

3. In this exercise we work over $\mathbb{Q}$, and revisit points of finite order again using reduction modulo p as a tool. The equation we are interested in is

$$C : y^2 = x^3 + bx \text{ for some nonzero } b \in \mathbb{Z}.$$

Let $\Phi \subset C(\mathbb{Q})$ be the subgroup consisting of all rational points of finite order on C.

(a) In Exercise 4.8, p. 142, it is shown that if p is any prime number such that $p \equiv 3 \pmod 4$, and b is not equal to 0 in $\mathbb{F}_p^*$, then the curve $C : y^2 = x^3 + bx$ satisfies $\#C(\mathbb{F}_p) = p + 1$. Assume this without proof, and use it to show that the order of the group Φ is 2 or 4.

(b) Recall from section III.4 that the multiplication by 2 map on C is decomposed as a composition $\psi \circ \phi$ where $\phi : C \to \overline{C}$ and $\psi : \overline{C} \to C$ are given by explicit formulas on p. 79. Use these formulas to show that there exists a rational point $P \in C$ such that $2P = (0, 0)$ if and only if $b = 4d^4$ for some integer d.

(c) Show that the group structure of Φ is given precisely by the following table:

$$\Phi = \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{if } b = 4d^4 \text{ for some } d \in \mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{if } -b \text{ is a square} \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$