18.704 Fall 2004 Homework 3

Due 10/8/04

All references are to the textbook “Rational Points on Elliptic Curves” by Silverman and Tate, Springer Verlag, 1992.

We are going to prove the following result in class:

Theorem 0.1 *Let C be a nonsingular curve $y^2 = x^3 + ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}$ are integers. Then if $P = (x, y)$ is a rational point of finite order on C, then x and y are both in $\mathbb{Z}$.*

Although we won't have finished proving this by the time you work on this problem set, for now assume the theorem above is true.

In all of the problems below, C will be a nonsingular cubic curve in Weierstrass normal form, i.e. the solution set to $y^2 = f(x) = x^3 + ax^2 + bx + c$ where $f(x)$ has distinct roots. We always take the zero element of the group to be the point at infinity $\mathcal{O} = [0, 1, 0]$.

1. For each curve below, determine if the given point has finite order, and if it does, calculate its order. Hint: rather than calculating $P, 2P, 3P, \ldots$, it might save time to calculate $P, 2P, 4P, 8P, \ldots$ and look for a pattern—note that the book gives an explicit doubling formula on p.31 (at least for the x-coordinate.)

(1) $y^2 = x^3 - 43x + 166$, $P = (3, 8)$.

(2) $y^2 = x^3 + 17$, $P = (-2, 3)$.

2. In this problem you will prove the strong form of the Nagell-Lutz Theorem, *assuming* Theorem 0.1 above. Assume that the equation of the nonsingular cubic curve $C : y^2 = f(x) = x^3 + ax^2 + bx + c$ has *integer* coefficients, i.e. $a, b, c \in \mathbb{Z}$. Let

$$\phi(x) = x^4 - 2bx^2 - 8cx + (b^2 - 4ac).$$

Recall from p. 31 of the text that if $P = (x, y)$ and we write $2P = (x', y')$ then $x' = \phi(x)/4y^2$. Let $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ be the discriminant of $f(x)$. Now it turns out to be true that there are polynomials $F(x)$, $\Phi(x)$ with integer coefficients such that

$$F(x)f(x) + \Phi(x)\phi(x) = D.$$

You can assume this without proof; it is tedious to determine F and Φ by hand.

(1) (Strong form of the Nagell-Lutz Theorem) Do Exercise 2.11(b) from the text.

(2) What is the minimum number of rational points of finite order that a nonsingular cubic curve in Weierstrass form can have (remember to count $\mathcal{O}$)? Find choices of $a, b, c \in \mathbb{Z}$ so that $y^2 = f(x)$ has this minimal number of them.

3. In this problem we allow the coefficients a, b, c of $f(x)$ to lie in the real numbers $\mathbb{R}$. We saw in class that $C : y^2 = f(x)$ has 9 points of order dividing 3 if one allows complex coefficients. In this problem we are going to see how many of these points have real coefficients. Recall from p. 40 of the text that a point $P = (x, y) \neq \mathcal{O}$ on C has order 3 if and only if x is a root of the polynomial

$$\psi(x) = 2f''(x)f(x) - f'(x)^2 = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2).$$

Now do Exercise 2.2(b) from the text.