18.704 Fall 2004 Homework 3 Solutions

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.

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 $P, 2P, 3P, \dots$, it might save time to calculate $P, 2P, 4P, 8P, \dots$ 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) $y^2 = x^3 + 17$, $P = (-2, 3)$.

Solution. Recall the formulas for doubling a point. Given $P = (x_0, y_0)$, the tangent line to C at P is $y = \lambda x + \nu$ where $\lambda = f'(x_0)/2y_0$ and $\nu = y_0 - \lambda x_0$. Then writing $2P = (x_1, y_1)$, we have $x_1 = \lambda^2 - a - 2x_0$ and $y_1 = -(\nu + \lambda x_1)$.

(1) In this part we have $a = 0, b = -43, c = 166$, and $P = (3, 8)$. Using the formulas above we can show that the tangent line to P is $y = -x + 11$, and $2P = (-5, -16)$. The tangent line to $2P$ is $y = -x - 21$, and $4P = (11, 32)$. The tangent line to $4P$ is $y = 5x - 23$, and $8P = (3, 8)$.

We notice that $8P = P$. This means that $7P = \mathcal{O}$. Thus P has finite order, and its order must divide 7, so it is 1 or 7. Since $\mathcal{O}$ is the only point of order 1 and $P \neq \mathcal{O}$, we must have that P has order 7.

(2) We use the same formulas, but now with $a = b = 0, c = 17$, $P = (-2, 3)$. Then the tangent line at P is $y = 2x + 7$, and $2P = (8, 23)$. Continuing, the

slope of the tangent line at $2P$ is $\lambda = 192/23$. We need go no farther; it is clear from the formulas above that $4P$ will not have integer x-coefficient. If P were a point of finite order, then $4P$ would also have finite order, and Theorem 0.1 would then imply that $4P$ has integer coefficients. Since this doesn't happen, we conclude that P has infinite order in the group.

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.

Solution. (1) By Theorem 0.1, if $P = (x_0, y_0)$ is a rational point of finite order then P has integer coefficients. If P has order 2 then the tangent line at P is vertical and $2P = \mathcal{O}$. Now assume that P is of finite order greater than 2 (in particular, then we know that $y_0 \neq 0$). Then we can use our given formulas, and $2P = (x_1, y_1)$ where $x_1 = \phi(x_0)/4y_0^2$. We have that $2P$ also has finite order, so it has integer coefficients by our theorem. Then x_1 is an integer and so in particular $y_0^2 | \phi(x_0)$. But since P is on the curve $y^2 = f(x)$, we certainly have $y_0^2 | f(x_0)$. Now we use the given information: there exist integer polynomials F, Φ such that

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

Plugging in x_0, we have

$$F(x_0)f(x_0) + \Phi(x_0)\phi(x_0) = D,$$

and since F, f, Φ, ϕ are all polynomials with integer coefficients, all of the quantities $F(x_0), f(x_0), \Phi(x_0), \phi(x_0)$ are integers. Since $y^2 | f(x_0)$ and $y^2 | \phi(x_0)$, we conclude from the equation that $y^2 | D$ as required.

(2). None of our results seem to force a curve in Weierstrass form to have any rational points whatsoever, except for the point $\mathcal{O}$. So we guess that C can have as only a single rational point of finite order. By playing around, we come up with the equation $C : y^2 = x^3 - 2$ (you will likely think up a different example.) Let us prove it has no rational points of finite order except $\mathcal{O}$. To be perfectly rigorous, I suppose we should check that C is nonsingular. Setting $f(x) = x^3 - 2$, we have $f'(x) = 3x^2$. Now the only root of $f'(x)$ is 0, which is not a root of f. By a previous homework problem, C is nonsingular.

Now it is easy to see that $x^3 - 2 = 0$ has no rational solutions for x, since any such solution would have to be an integer dividing 2. So C has no rational points of order 2. Now suppose C has a rational point (x_0, y_0) of finite order > 2. Then x_0, y_0 are integers. The discriminant of f is $D = -4(27)$. By the strong form of the Nagell-Lutz theorem, $y_0^2| - 108$. Then $y_0 = \pm1, \pm2, \pm3$, or ±6. However, none of the equations $x^3 - 2 = 1, 4, 9, 36$ has any integer solution for x, since $3, 6, 11$, and 38 are not cubes. Thus C has no rational points of finite order in the affine plane, so $\mathcal{O}$ is its only rational point.

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.

Solution. We saw in class that $\psi(x)$ has 4 distinct roots (over the complex numbers.) Consider the local extrema of ψ; these occur at points x where $\psi'(x) = 0$. Also, we note that $\psi'(x) = 12f(x)$.

By the mean value theorem, between any two values $\alpha_1 < \alpha_2$ such that $\psi(\alpha_1) = \psi(\alpha_2) = 0$, there must be a $\alpha_1 < \beta < \alpha_2$ with $\psi'(\beta) = 0$. In other words, between any two zeroes of ψ lies a local extremum.

Now suppose α is a value such that $\psi(x)$ has a local extremum at α, so $\psi'(\alpha) = 12f(\alpha) = 0$, and so $f(\alpha) = 0$. Then $\psi(\alpha) = -f'(\alpha)^2 \leq 0$. Moreover, if $\psi(\alpha) = 0$, then $f'(\alpha) = 0$, so that f and f' have a common root α, contradicting the fact that the curve C is assumed to be nonsingular. Thus actually $\psi(\alpha) < 0$ at any value of α where ψ has a local maximum or minimum. But since the leading term of $\psi(x)$ is $3x^4$, we definitely have that $\lim_{x\to\infty} \psi(x) = \infty$ and $\lim_{x\to-\infty} \psi(x) = \infty$.

From all of this, we conclude that ψ has precisely two real roots, say $\alpha_1 < \alpha_2$, and that $\psi(a) < 0$ for all $\alpha_1 < a < \alpha_2$, with all of the local extrema occurring in this range. In particular, ψ is decreasing at $x = \alpha_1$ and increasing at $x = \alpha_2$. Since $\psi' = f$, we see that $f(\alpha_1) < 0 < f(\alpha_2)$.

Then the points of order 3 with real x-coordinate are $(\alpha_1, \pm\sqrt{f(\alpha_1)})$ and $(\alpha_2, \pm\sqrt{f(\alpha_2)})$. But only the two points $(\alpha_2, \pm\sqrt{f(\alpha_2)}$ have real y-coordinate.

Together with $\mathcal{O}$, these form exactly 3 points of order dividing 3 with coefficients in $\mathbb{R}$.