18.704 Fall 2004 Homework 4 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.

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.)

Solution. (with thanks to Emmanuel Stoica.) Notice that as in the book we use (t, s)-coordinates, i.e. we let the t-axis be horizontal and the s-axis be vertical (I'm not sure why this is the convention.) Also, we assume that a, b, c are integers, since all of Section II.4 is under this assumption.

Fix a prime p and define $\operatorname{ord}(r)$ for each rational number r as in the book. Note that another way of describing $C(p^\nu)$ is as the ordered pairs (t, s) on the curve for which $\operatorname{ord}(t) \geq \nu$ and $\operatorname{ord}(s) \geq 3\nu$.

First suppose that $P_1 * P_2 = Q$ is a point at infinity. Since the line ℓ through $P_1 * P_2$ is vertical, we would have to have $Q = [0, 1, 0]$ in projective T, S, U-coordinates. From the homogeneous equation

$$U^2S = T^3 + aT^2S + bTS^2 + cS^3,$$

this happens if and only if $c = 0$.

We claim the case above never occurs, as follows. Under our change of coordinates, the point Q corresponds to the point $(0, 0)$ in (x, y)-coordinates. In the (x, y)-plane, the point $(0, 0)$ is a point of order two, and the tangent line to the curve at the point $(0, 0)$ is $x = 0$. Then in the (t, s)-plane, the point Q

also has order 2 and since the change of coordinates is $t = x/y, s = 1/y$, the tangent line to the curve at Q must be the line $t = 0$. This is a vertical line, so it must be the line ℓ itself. But ℓ hits the curve at least twice at Q (since it is tangent at Q) and so ℓ cannot also contain two other points P_1, P_2 on the curve. This contradiction eliminates this case.

From now on we can assume that $c \neq 0$, and that $P_1 * P_2 = (t_3, s_3)$ is not a point at infinity. Since the line through P_1 and P_2 is vertical, clearly $t_3 = t_1 = t_2$. Now since the equation of C in (t,s)-coordinates has only odd powers of t and s, the curve is symmetric about the origin, i.e. if $(t,s) \in C$ then $(-t,-s) \in C$. Since we take $\mathcal{O} = (0,0)$, then from the symmetry it is clear that $(t,s) * \mathcal{O} = (-t,-s)$. So $P_1 + P_2 = (-t_3, -s_3)$, and obviously $\operatorname{ord}(-t_3) = \operatorname{ord}(-t_1) = \operatorname{ord}(t_1) \geq \nu$. It remains to prove that $\operatorname{ord}(s_3) \geq 3\nu$.

Now, the 3 s-coordinates s_1, s_2, s_3 are the three roots of the equation

$$cs^3 + bt_1 s^2 + (at_1^2 - 1)s + t_1^3 = 0.$$

Thus $(-b/c)t_1 = s_1 + s_2 + s_3$. Since $\operatorname{ord}(s_1) \geq 3\nu$ and $\operatorname{ord}(s_2) \geq 3\nu$, we just need to prove that $\operatorname{ord}(-b/c)t_1 \geq 3\nu$.

Now write $t = t_1$ for convenience. Since $s_i = t^3 + at^2 s_i + bts_i^2 + cs_i^3$ for each i, we can subtract and factor some terms to get

$$s_1 - s_2 = at^2(s_1 - s_2) + bt(s_1 - s_2)(s_1 + s_2) + c(s_1 - s_2)(s_1^2 + s_1 s_2 + s_2^2).$$

Cancelling the factor $s_1 - s_2$ (OK since we assumed $P_1 \neq P_2$) and solving for c, we have

$$c = (1 - at^2 - bt)/(s_1^2 + s_1 s_2 + s_2^2), \text{ so } bt/c = bt(s_1^2 + s_1 s_2 + s_2^2)/(1 - at^2 - bt).$$

The presence of the 1 in the denominator implies (since we know $\operatorname{ord}(t) \geq 1$) that $\operatorname{ord}(1 - at^2 - bt) = 0$. On the other hand, we have $b \in \mathbb{Z}$, $\operatorname{ord} t \geq \nu$, and $\operatorname{ord}(s_1^2 + s_1 s_2 + s_2^2) \geq 6\nu$. So certainly $\operatorname{ord}(bt/c) \geq 3\nu$ as we wished.

2. Do Exercise 2.10 from the textbook.

Solution. Let C be the curve $y^2 = x^3 + px$ where p is a prime number. First we find the points of order 2. These are the points $(x, 0)$ on the curve, so that $x(x^2 + p) = 0$. Since p is prime, $x^2 + p = 0$ has complex roots, so $(0,0)$ is the only point of order 2. Of course $\mathcal{O} = [0,1,0]$ is always point of order 1.

Now if (x,y) is a point of finite order > 2, then the strong form of the N-L Theorem, which you proved in Homework 3, says that x and y are integers, and $y^2 | D$, where here $D = -4p^3$. hence $y = \pm 1, \pm 2, \pm p$, or $\pm 2p$.

Since $y^2 > 0$ and $p > 0$, we have $x > 0$. Since $x \geq 1$ and $p \geq 2$, $x^3 + px \geq 3$, so $y \neq \pm 1$.

Suppose $y = \pm 2$. Then if $x \geq 2$ then since $p \geq 2$, $x^3 + px \geq 12$, a contradiction. So $x = 1$ is the only possible case here, which forces $p = 3$. So we have identified some possible candidates for points of finite order:

$$p = 3 : \quad (1,2), (1,-2).$$

We are left with the cases $y = \pm p$ or $y = \pm 2p$. In either case $p^2 | y^2 = x(x^2 + p)$. So necessarily either $p|x$ or $p|(x^2 + p)$. But in the latter case, $p|x^2$, so $p|x$ in any case. But then $x(x^2 + p) \geq p(p^2 + p) > p^2$, so $y \neq \pm p$.

We are left with the case $y = \pm 2p$, so $4p^2 = x^3 + px \geq p^3 + p^2$, which forces $3p^2 \geq p^3$, and so $p \leq 3$ and $p = 2$ or 3. If $p = 2$, then $16 = x^3 + 2x$ is readily seen to have no integer solutions. If $p = 3$, then we check that $36 = x^3 + 3x$ has only the integer solution $x = 3$. So we have a few more possible candidates for points of finite order:

$$p = 3 : \quad (3, 6), (3, -6).$$

So we now assume that $p = 3$; we need to check if any of the points

$$P = (1, 2), \quad Q = (3, 6), \quad -P, \quad -Q$$

has finite order on the curve $y^2 = x^3 + 3x$. The tangent line at P has slope $6/4 \notin \mathbb{Z}$, so it follows that $2P$ will not have integer coordinates. The tangent line at Q has slope $30/12 \notin \mathbb{Z}$, so $2Q$ will also not have integer coordinates. By the N-L theorem, neither P nor Q has finite order. But then $-P$ and $-Q$ also do not have finite order.

So overall, we have proven that regardless of p, the group of rational points of finite order on C is precisely

$$\{\mathcal{O}, (0, 0)\}.$$

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.)

Partial Solution. This problem is potentially very difficult, but I thought it might be fun for you to play with. Once we develop some more techniques, we will be able to solve this in full more easily. So I will not give the entire solution here at this point.

For part (a), we note that Exercise 3.7(c) claims that the group of points of finite order on $C : y^2 = x^3 + dx$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ if $d = e^4$ for some integer e.

But if $e = 1$, then we have the curve $y^2 = x^3 + x$. This has 2 points of order dividing 2, namely $\{\mathcal{O}, (0, 0)\}$. But the discriminant D in this case is -4, so if (x, y) has finite order, then $y = \pm 1, \pm 2$ by the strong form of Nagell-Lutz. But $1 = x^3 + x$ and $4 = x^3 + x$ are readily seen to have no integer solutions. It follows that C has no points of finite order except those of order dividing two, and that the full group of points of finite order is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. so the table in Exercise 3.7(c) cannot possibly be correct.

For part (b), it turns out that the other parts of the table are correct, but that the first line of the table should say the the group of points of finite order on $C : y^2 = x^3 + dx$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ if $d = 4e^4$ for some integer e. In fact, Exercise 4.9 has the correct statement (although it phrases it differently, by assuming that d is not divisible by any fourth power. Actually, it is possible to reduce to this case.)

As for (c), we'll hopefully see how to do this at a later date.