18.704 Fall 2004 Homework 2 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. A cubic in Weierstrass normal form is $C_0 : y^2 = x^3 + ax^2 + bx + c$, or in homogeneous coordinates, $C : Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$. Prove that C is a nonsingular curve if and only if the polynomial $x^3 + ax^2 + bx + c$ has distinct roots. Show also that the point at infinity $[0, 1, 0]$ is an inflection point on the curve C.

Solution. We will solve this problem using homogeneous coordinates.

(*Note*: the book does prove on p. 26 that C_0 has a singular point if and only if $f(x) = x^3 + ax^2 + bx + c$ has distinct roots. So another approach is to reproduce that "affine coordinates" proof; then you only need to show that the single point at infinity $[0, 1, 0]$ is always nonsingular.)

Let $F(X, Y, Z) = X^3 + aX^2Z + bXZ^2 + cZ^3 - Y^2Z$, so that C is the vanishing locus in $\mathbb{P}^2$ of the polynomial F. Suppose that $[r, s, t]$ is a point on the curve where all three partial derivatives of F vanish. We calculate

$$\partial F/\partial X = 3X^2 + 2aXZ + bZ^2$$
$$\partial F/\partial Y = 2YZ$$
$$\partial F/\partial Z = aX^2 + 2bXZ + 3cZ^2 - Y^2.$$

From the second equation we see that either $s = 0$ or $t = 0$. Suppose that $t = 0$; then the first equation gives $r = 0$, and finally the third equation gives $s = 0$. But $[0, 0, 0]$ is not a point in $\mathbb{P}^2$, so we can ignore this possibility.

This means that we do not have to worry about the case $t = 0$, so since we are working in projective space we can assume that $t = 1$ by scaling. We still have to worry about the case $s = 0$. In that case, the first equation above says that r is a root of $3x^2 + 2ax + b = 0$. Since $[r, 0, 1]$ also lies on the curve C, r is a root of $x^3 + ax^2 + bx + c = 0$. Thus r is a root both of the polynomial $p(x) = x^3 + ax^2 + bx + c$ and its derivative $p'(x) = 3x^2 + 2ax + b$. Then r is a double root of the polynomial $p(x)$ and $p(x)$ does not have distinct roots.

Conversely, if r is a multiple root of the polynomial $p(x)$ then r is also a root of the polynomial $p'(x)$. But then r is also a root of $3p(x) - xp'(x) = ax^2 + 2bx + 3c$. It follows that in this case $[r, 0, 1]$ is a point on C where all three partial derivatives vanish, so C fails to be nonsingular.

To show that $P = [0, 1, 0]$ is an inflection point on C, we first need to find the tangent to the curve C at P. This is the line $\alpha X + \beta Y + \gamma Z = 0$ where $\alpha = \partial F/\partial X(P) = 0$, $\beta = \partial F/\partial Y(P) = 0$, and $\gamma = \partial F/\partial Z(P) = -1$. In other words, the line at infinty $Z = 0$ is the tangent line to C at the point P. But since P is clearly the only point of intersection of $Z = 0$ with C, the point P must be an inflection point.

2. Let C be a nonsingular cubic curve in $\mathbb{P}^2$ (not necessarily in Weierstrass form.) Suppose that $\mathcal{O}$ is an inflection point on C. Make the rational points on C into a group using $\mathcal{O}$ as the identity element, as in Section I.2 of the text.

(a) Prove that a point $P \in C$ satisfies $P+P = \mathcal{O}$ (in other words the order of P in the group divides 2) if and only if the tangent line to C at P goes through $\mathcal{O}$.

(b) Prove that a point $P \in C$ satisfies $P + P + P = \mathcal{O}$ (i.e. P has order dividing 3 in the group) if and only if P is an inflection point on the curve.

Solution. (a) We have $P + P = (P * P) * \mathcal{O}$. If $P + P = \mathcal{O}$, then there is a line ℓ whose three points of intersection with C are $\mathcal{O}, \mathcal{O}, P * P$. Since ℓ hits $\mathcal{O}$ twice, ℓ must be the tangent line to C at $\mathcal{O}$. But since $\mathcal{O}$ is a point of inflection, this happens if and only if $P * P = \mathcal{O}$. This says exactly that the tangent line to the curve at P goes through $\mathcal{O}$. The converse is similar.

(b) Recall the way we constructed additive inverses to show that the points on C are a group: first find $\mathcal{O} * \mathcal{O}$; In our case this is $\mathcal{O}$ again. Then given any point P on C, we have $-P = P * \mathcal{O}$.

Now suppose that $P+P+P = (P+P)+P = \mathcal{O}$. Then $P*\mathcal{O} = -P = P+P$. Write $Q = P * P$. Then $P * \mathcal{O} = P + P = \mathcal{O} * Q$; this means the line through P and $\mathcal{O}$ and the line through Q and $\mathcal{O}$ have identical third points of intersection, which forces $P = Q$. Finally, we have shown $P * P = P$ which means that P is an inflection point.

The converse follows by reversing these steps.

3. This problem concerns the affine curve $C_0 : x^3 + y^3 = \alpha$ for some nonzero constant α. In homogeneous coordinates, this is $C : X^3 + Y^3 = \alpha Z^3$. In particular, $[1, -1, 0]$ is a point at infinity on the curve. In fact C is a nonsingular curve and $[1, -1, 0]$ is an inflection point (you don't have to prove this.) Define a group law on C by taking $\mathcal{O} = [1, -1, 0]$ as the identity.

(a) Given a point $P = (x_0, y_0) \in C_0$, find the tangent line to C at P.

(b) Let $P = (x_0, y_0)$ be a rational point on C_0. Find the coordinates of the additive inverse Q of P, that is, the point Q such that $P + Q = \mathcal{O}$.

(c) Find all of the complex points P on C such that $P + P = \mathcal{O}$. There are four. How many of these points are rational points? (The answer depends on α.)

(d) Let $\alpha = 9$. Then $(1, 2) \in C_0$. Calculate $(1, 2) + (1, 2)$. (You don't need to use section I.4. The formulas there are not applicable because they assume the curve is in Weierstrass form.)

(e)* Let $\alpha = 1000$. find *all* of the rational points on C in this case (feel free to quote known theorems without proof.) What kind of group do we get for the set of all rational points on C?

Solution. (a) Using implicit differentiation, we have

$$3x^2 + 3y^2\frac{dy}{dx} = 0, \text{ so that } \frac{dy}{dx} = -\frac{x^2}{y^2}.$$

Then the tangent line to C_0 at (x_0, y_0) is

$$y - y_0 = -\left(\frac{x_0^2}{y_0^2}\right)(x - x_0).$$

(b) Since $\mathcal{O}$ is an inflection point, as we saw in problem 2 above we have $-P = P * \mathcal{O}$. Since $\mathcal{O}$ is the point at infinity coresponding to the direction $(1, -1)$, the line through P and $\mathcal{O}$ is the unique line ℓ through P with slope -1, i.e. the line $(y - y_0) = -(x - x_0)$. But since the curve C_0 is symmetric about the line $y = x$, it follows that ℓ hits C_0 in the third point (y_0, x_0). (If this geometric argument bothers you, one can also see this algebraically.) So $-P = (y_0, x_0)$.

(c) From problem 2 above, we are looking for all points P such that $P * P = \mathcal{O}$. We know that $\mathcal{O}$ itself is one such point, so assume now that $P \neq \mathcal{O}$. Then $P = (x_0, y_0)$ is on the affine part of the curve C_0. We calculated the tangent line to the curve at P above in part (a). This line will contain the point $\mathcal{O}$ if and only if it has slope -1, i.e. if and only if $x_0^2 = y_0^2$, or $x_0 = \pm y_0$. Note that we can't have $x_0 = -y_0$, for then since $(x_0, y_0) \in C$, we would have $\alpha = 0$, which we excluded.

So any point of order dividing 2 on the curve has the form (x_0, x_0). Then $x_0^3 = \alpha/2$. If we define $\gamma = \sqrt[3]{\alpha/2}$, then the solutions to this equation are

$$x_0 = \gamma,\ \gamma\delta,\ \gamma\delta^2$$

where $\delta = -1/2 + \sqrt{3}i/2$ is a third root of 1. Thus we have found all of the points of order 2 on the curve:

$$\mathcal{O} = [1, -1, 0], \quad (\gamma, \gamma), \quad (\gamma\delta, \gamma\delta), \quad (\gamma\delta^2, \gamma\delta^2).$$

$\mathcal{O}$ is definitely a rational point on the curve (its homogeneous coordinates are certainly rational.) Since γ is real, $\gamma\delta$ and $\gamma\delta^2$ cannot be real numbers, so they are certainly not rational. Thus the only other point that is potentially rational is (γ, γ), which is rational if and only if α happens to be twice the cube of a rational number.

To summarize: if α is twice the cube of a rational number, then C has two rational points of order dividing 2, namely (γ, γ) and $\mathcal{O}$; on the other hand, if α is not twice the cube of a rational number, then $\mathcal{O}$ is the only rational point on C of order dividing 2.

(d) Now let $\alpha = 9$. The tangent line at the point $(1, 2)$ is

$$(y - 2) = (-1/4)(x - 1),$$

by part (a). To find its third intersection point with C, we substitute $y = (-1/4)x + 9/4$ into the equation for C, getting

$$\begin{gathered} x^3 + ((-1/4)x + 9/4)^3 = 9, \\ 63/64x^3 + 27/64x^2 + a_1 x + a_2 = 0, \\ x^3 + 3/7x^2 + b_1 x + b_2 = 0, \end{gathered}$$

where here a_1, a_2, b_1, b_2 are some constants we won't care about. Then the sum of the three roots of the cubic is (-3/7), and so since the root $x = 1$ has multiplicity two we must have the third root is $x_3 = -3/7 - 1 - 1 = -17/7$. Then the corresponding y-coordinate is $y_3 = (-1/4)(-17/7) + 9/4 = 20/7$. Thus $P * P = (-17/7, 20/7)$. Then $P + P = (P * P) * \mathcal{O}$, which as we saw in part (b) is equal to

$$P + P = (20/7, -17/7).$$

(e) Since $\alpha = 1000$, we are looking for rational solutions to $x^3 + y^3 = 10^3$. If we write $x = X/Z$, $y = Y/Z$ for some integers X, Y, Z, then $X^3 + Y^3 = (10Z)^3$. Now if we quote Fermat's last theorem for the case of the exponent 3 (that case has been known for many years), then it says that the only solutions to this equation are the ones where one of X, Y, Z is 0. Since Z can't be zero, we see that the only possible solutions are $X = 0, Y = 10Z$, or $X = 10Z, Y = 0$. In affine coordinates these are the two trivial solutions $(x, y) = (0, 10), (10, 0)$. But we need to also include the point at infinity $[1, -1, 0]$, which is always a rational point on the curve C (regardless of α.) So the group of rational points on C consists of precisely 3 elements. There is only one such group up to isomorphism, namely the cylic group of order 3.