# 18.704 Fall 2004 Homework 1 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.** Do Exercise A.3 from the textbook, parts (a) and (b).

**Solution.** (a) Think of $\mathbb{P}^2$ as

$$\{[a,b,c] | a,b,c \text{ not all zero}\}/\sim$$

where $[a,b,c] \sim [a',b',c']$ if there exists a nonzero $t$ with $a = ta', b = tb', c = tc'$.

Now let $x, y, z$ be coordinates in 3-space, i.e. $\mathbb{A}^3$. We define a map

$$\theta : \text{Lines in } \mathbb{A}^3 \text{ through the origin} \longrightarrow \mathbb{P}^2$$

as follows. Given a line $\ell$ through the origin in $\mathbb{A}^3$, simply pick any point $(a,b,c) \neq (0,0,0)$ on $\ell$ and define $\theta(\ell) = [a,b,c] \in \mathbb{P}^2$. Why is this well-defined? Well if we pick a different non-origin point $(a',b',c') \in \ell$ then since $\ell$ is a line through the origin, $(a',b',c')$ is just a nonzero scalar multiple of $(a,b,c)$, so $[a',b',c'] = [a,b,c] \in \mathbb{P}^2$.

The map $\alpha$ is surjective: given $p = [a,b,c] \in \mathbb{P}^2$, then the vector $(a,b,c) \neq (0,0,0)$ and so $p = \alpha(\ell)$ where $\ell$ is the unique line joining $p$ to the origin. The map $\alpha$ is injective: if $\alpha(\ell_1) = [a,b,c] = \alpha(\ell_2)$, then both of the points $(0,0,0), (a,b,c)$ lie on both of the lines $\ell_1, \ell_2$, so since two points determine a unique line we have $\ell_1 = \ell_2$. Thus $\alpha$ determines a bijective correspondence between lines in $\mathbb{A}^3$ through the origin and points in $\mathbb{P}^2$.

(b) Every plane $\Gamma$ through the origin in $\mathbb{A}^3$ has the form

$$\Gamma_{\alpha,\beta,\gamma} = \{(a,b,c) \in \mathbb{A}^3 | \alpha a + \beta b + \gamma c = 0\}$$

for some $\alpha, \beta, \gamma$ not all zero. But by our definition of lines in $\mathbb{P}^2$, every line $\ell \in \mathbb{P}^2$ has the form

$$\ell_{\alpha,\beta,\gamma} = \{[a,b,c] \in \mathbb{P}^2 | \alpha a + \beta b + \gamma c = 0\}$$

for some $\alpha, \beta, \gamma$ not all zero.

Since

$$\alpha(S_{\Gamma_{\alpha,\beta,\gamma}}) = L_{\Gamma_{\alpha,\beta,\gamma}} = \ell_{\alpha,\beta,\gamma},$$

there is a bijective correspondence between planes $\Gamma$ through the origin in $\mathbb{A}^3$ and lines in $\mathbb{P}^2$.

**2.** Do Exercise A.8 part (b) from the text.

**Solution.** Let $C_0$ be the affine curve $x^2 + xy - 2y^2 + x - 5y + 7 = 0$. Since the largest degree of the terms in the equation for $C_0$ is 2, we may homogenize the equation by adding enough powers of $Z$ to each term to make it have degree 2. So we get that

$$C : X^2 + XY - 2Y^2 + XZ - 5YZ + 7Z^2 = 0$$

defines a curve in $\mathbb{P}^2$ whose affine part is the given affine curve $C_0$. To find the points at infinity on $C$, we substitute $Z = 0$ and solve:

$$X^2 + XY - 2Y^2 = 0.$$

Factoring, we have

$$(X + 2Y)(X - Y) = 0, \text{ so } X = -2Y \text{ or } X = Y.$$

Thus there are two points at infinity on $C$, $[-2, 1, 0]$ and $[1, 1, 0]$. These correspond to the "directions" in the affine plane given by the lines $x = -2y$ and $x = y$.

**3.** (a) Do Exercise A.16(a) from the textbook.

(b) **(*)** Do Exercise A.16(b) from the textbook.

**Solution.** (a) The equation of an arbitrary conic in $\mathbb{P}^2$ takes the form

$$C : aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0$$

for some $a, b, c, d, e, f$ not all zero. Suppose we pick a random point in $\mathbb{P}^2$, such as $P = [2, 3, 5] \in \mathbb{P}^2$. Then $P$ lies on $C$ if and only if $4a+6b+9c+10d+15e+25f = 0$. Similarly, given any point $P_i = [r_i, s_i, t_i] \in \mathbb{P}^2$, the condition for $p$ to lie on $C$ is a single linear equation $r_i^2 a + r_i s_i b + s_i^2 c + r_i t_i d + s_i t_i e + t_i^2 f = 0$. Thus we see that the 5 given points $P_1, \ldots, P_5$ lie on $C$ if and only if $r_i^2 a + r_i s_i b + s_i^2 c + r_i t_i d + s_i t_i e + t_i^2 f = 0$ holds for $i = 1, 2, \ldots, 5$. Since this is a set of 5 homogeneous equations in the 6 variables $a, b, c, d, e, f$, there is at least one solution for $a, b, c, d, e, f$ with not all of them zero.

(b) In this problem, one is supposed to show that there is a unique conic going through the 5 distinct points if and only if no four of the five points lie on a line. This was an extra credit problem and the proof is a little involved; please come see me if you want to talk over the solution.

**4.** Do Exercise 1.7 parts (b) and (c) from the text. Also, in case some rational point exists, find formulas which give all rational points in terms of a parameter $t$, and use the formula to write down some particular rational point on the curve that you would have never guessed by inspection.

*Solution.* (a) We will show that there are no rational solutions to the equation $3x^2 + 5y^2 = 4$. Suppose that $(x, y)$ is a rational solution to the equation. We can choose a common denominator for the rational numbers $x, y$ so that $x = X/Z$, $y = Y/Z$, with $X, Y, Z$ integers. Then $[X, Y, Z]$ lies on the projective curve $C : 3X^2 + 5Y^2 - 4Z^2 = 0$.

Recall the notation $a|b$ means that "$a$ divides $b$". If there is some integer $p$ such that $p|X$, $p|Y$, and $p|Z$, then $[X', Y', Z']$ is also on the curve $C$, where $X' = X/p$, $Y' = Y/p$, $Z' = Z/p$. Thus by removing all common factors from $[X, Y, Z]$ we may assume that $[X, Y, Z]$ is a point on the curve such that $\gcd\{X, Y, Z\} = 1$.

Now any square is congruent to either 0 or 1 modulo 3. Then $3X^2 \equiv 0 \mod 3$, $5Y^2 \equiv 0$ or $2 \mod 3$, and $4Z^2 \equiv 0$ or $1 \mod 3$. The only way this is possible is if $3X^2 \equiv 5Y^2 \equiv 4Z^2 \equiv 0 \mod 3$. But then $3|Y$ and $3|Z$. Consequently, $9|Y^2$ and $9|Z^2$, forcing $3|X$. Now $X, Y, Z$ have the common factor 3, contradicting the assumption that $\gcd\{X, Y, Z\} = 1$. This contradiction proves that the original curve cannot have a rational point.

(b) By trial and error, we find the point $(2/3, 2/3)$ is a rational point on the curve $C_0 : 3x^2 + 6y^2 = 4$. Now we follow the method on page 11 of the text for parametrizing the rational points on the curve. Given the point $(0, t)$ with $t$ rational, the line through $(2/3, 2/3)$ and $(0, t)$ is $y = t + (2 - 3t)(x)/2$. This hits the curve $C_0$ at an additional point $(x_0, y_0)$. Substituting the formula for $y$ into the equation for $C_0$, we get a quadratic equation in $x$:

$$x^2 + \frac{-12t^2 + 8t}{9t^2 - 12t + 6}x + \text{constant term } = 0.$$

Since one of the roots is $x = 2/3$, the other is

$$x_0 = \frac{12t^2 - 8t}{9t^2 - 12t + 6} - 2/3$$

and then

$$y_0 = t + (2 - 3t)(x_0)/2.$$

(*Note.* Your exact formulas may be different depending on your choice of a rational line on which to project.)

Now letting $t$ run over all rational numbers, $(x_0, y_0)$ defined by these formulas runs over all rational points on the curve $C_0$. (Actually, one point is missed. We need to let "$t = \infty$" in order to get the point $(2/3, -2/3)$.)

Picking $t = 1$, we get $(x_0, y_0) = (2/3, 2/3)$ again! But picking $t = -1$ we get the more interesting point $(2/27, -22/27) \in C_0$ which is a point we would have been unlikely to guess.