Homework Assignment 7: Elliptic Curves I
Due Wednesday November 20

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2002**

Instructions: *Please work with others, and feel free to use a computer, especially on problem 4.* (There are **7 problems.**)

1. We call a line in $\mathbb{C}^2$ *rational* if it is the set of zeros of an equation $ax + by + c = 0$ with $a, b, c \in \mathbb{Q}$.

   (a) (1 point) Suppose P and Q are distinct elements of $\mathbb{Q}^2$. Prove that the unique line in $\mathbb{C}^2$ that contains P and Q is rational.

   (b) (2 points) Suppose that L_1 and L_2 are distinct rational lines in $\mathbb{C}^2$ that intersect. Prove that their intersection is a rational point.

2. (4 points) Let $Y \subset \mathbb{C}^2$ be the set of complex solutions (x, y) to the equation $y^2 = x^5 + 1$. Find (with proof!) the closure of Y in $\mathbb{P}^2$.

3. (3 points) Let E be the elliptic curve defined by $y^2 = x^3 + 1$. Find the divisor associated to the rational function $(x + 1)/(y - 1)$.

4. (6 points) Let x and y be indeterminates.

   (a) Prove that $\mathbb{C}[x, y]/(y^2 - (x^3 + 1))$ is integrally closed in $\mathbb{C}(x)[y]/(y^2 - (x^3 + 1))$. That is, if $f(x), g(x) \in \mathbb{C}(x)$ are rational functions in x and $f(x) + yg(x)$ satisfies a monic polynomial with coefficients in $\mathbb{C}(x)$, then $f(x)$ and $g(x)$ are polynomials.

   (b) Prove that $\mathbb{C}[x, y]/(y^2 - x^3)$ is *not* integrally closed in $\mathbb{C}(x)[y]/(y^2 - x^3)$. [Hint: Consider $t = y/x$.]

5. Let E be the elliptic curve defined by $y^2 = x^3 + x + 1$. Consider the points $P = (72 : -611 : 1)$, $Q = (1/4 : -9/8 : 1)$, and $R = (1 : \sqrt{3} : 1)$ on E.

   (a) (2 points) Compute the sum of P and Q on E.

   (b) (2 points) Find nonzero integers n and m such that $nP = mQ$.

   (c) (2 points) Compute $R + R$.

   (d) (3 points) Is there any integer n such that $nR = P$? (Hint: Keep in mind the automorphism $\sqrt{3} \mapsto -\sqrt{3}$ of $\mathbb{Q}(\sqrt{3})$.)

6. Let $g(t)$ be a quartic polynomial with distinct complex roots, and let α be a root of $g(t)$. Let $\beta \neq 0$ be any complex number.

   (a) (3 points) Prove that the equations

$$x = \frac{\beta}{t - \alpha} \qquad \text{and} \qquad y = x^2 u = \frac{\beta^2 u}{(t - \alpha)^2}$$

define an algebraic map from the curve $u^2 = g(t)$ (in $\mathbb{C}^2$) to the curve $y^2 = f(x)$ (in $\mathbb{C}^2$), where $f(x)$ is the cubic polynomial

$$f(x) = g'(\alpha)\beta x^3 + \frac{1}{2}g''(\alpha)\beta^2 x^2 + \frac{1}{6}g'''(\alpha)\beta^3 x + \frac{1}{24}g''''(\alpha)\beta^4.$$

(You just have to check that if (u, t) satisfies $u^2 = g(t)$ then (x, y) defined by the above equations satisfies $y^2 = f(x)$.)

(b) (3 points) Prove that since g has distinct complex roots, f also has distinct roots, so $u^2 = g(t)$ is an elliptic curve.

7. This problem is about the connection between elliptic curves and ellipses. Let α and β be positive real numbers with $\beta \leq \alpha$, and let C be the ellipse

$$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 1.$$

(a) (3 points) Prove that the arc length of C is given by the integral

$$4\alpha \int_0^{\pi/2} \sqrt{1 - k^2 \sin^2\theta}\, d\theta$$

for an appropriate choice of constant k depending on α and β.

(b) (1 point) Check your value for k in (i) by verifying that when $\alpha = \beta$, the integral yields the correct value for the arc length of a circle.

(c) (3 points) Prove that the integral in (i) is also equal to

$$4\alpha \int_0^1 \sqrt{\frac{1 - k^2t^2}{1 - t^2}}\, dt = 4\alpha \int_0^1 \frac{1 - k^2t^2}{\sqrt{(1 - t^2)(1 - k^2t^2)}}\, dt.$$

(d) (0 points) By Exercise 6, the equation

$$u^2 = (1 - t^2)(1 - k^2t^2)$$

determines an elliptic curve. Hence the problem of determining the arc length of an ellipse comes down to evaluating the integral

$$\int_0^1 \frac{1 - k^2t^2}{u} dt$$

on the elliptic curve determined by $u^2 = (1 - t^2)(1 - k^2t^2)$.