Math 7770 Spring 2011
Homework 7
Due: March 21, 2011

You are welcome to work together but everyone needs to write up **distinct** solutions. If you use any books outside of our textbook or other people, please make sure to give them credit. Make sure your solutions are complete. If your handwriting is atrocious, I am happy to give you a basic introduction to LaTeX.

Warmup

- (a) If P and Q are distinct rational points in the (x, y) plane, prove that the line connecting them is a rational line.

  (b) If L_1 and L_2 are distinct rational lines in the (x, y) plane, prove that their intersection is a rational point (or empty).

- §2.10 #1. Which of the following are groups? (See the book for the complete list).

- §2.10 #2. Let G have as elements the four pairs $(1, 1)$, $(1, -1)$, $(-1, 1)$. and $(-1, -1)$. Let the group operation be $(a, b) * (c, d) = (ac, bd)$, Prove that G is a group.

Problems

1. §5.6 # 2. Find a parametrization of the rational points on the hyperbola $x^2 - 2y^2 = 1$ starting from the point $(3, 2)$.

2. §5.6 # 5. Show that the curve $y^2 = x^3 + 2x$ has a double point. Find all rational points on this curve.

3. Find all the rational points on the circle $x^2 + y^2 = 2$ by projecting from the point $(1, 1)$ onto an appropriate rational line. (Hint: Your formulae will be simpler if you are clever in your choice of the line.)

4. Let G be a group.

   (a) Show that there is only one identity element in G.

   (b) Show that any $g \in G$ has only one inverse.

Challenge

On the next page are two problems which help explain why the cubic equations we talked about in class are called "elliptic" curves. These questions rely on some outside knowledge so if you want to work on them and need any clarification, feel free to ask.

I. 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 number.

(a) Prove that the equations

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

give a birational transformation between the curve $u^2 = g(t)$ and the curve $y^2 = f(x)$ where $f(x)$ is the cubic polynomial

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

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

II. Let $0 < \beta \leq \alpha$, and let E be the ellipse

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

(a) Prove that the arc length of E 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 the constant k depending on α and β.

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

(c) Prove that the integral in (a) 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) Prove that if the ellipse E is not a circle, then the equation

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

defines an elliptic curve (see the previous exercise). Hence the problem of determining the arc length of an ellipse comes down to evaluating the integral

$$\int_0^1 \frac{1-k^2t^2}{u}dt \text{ on the "elliptic" curve } u^2 = (1-t^2)(1-k^2t^2).$$