Homework 8: Elliptic Curves

Due Wednesday, November 21

William Stein

Math 124 Harvard University **Fall 2001**

There are **six problems**. Some of the problems involve tedious algebra, and in all such cases you are allowed to do that algebra using, e.g., PARI as long as you explain *how* you used the system to do the algebra. Problems 4, 5, and 6 are from Silverman and Tate's book *Rational Points on Elliptic Curves.*

1. (3 points) Consider the elliptic curve $y^2+xy+y=x^3$ over $\mathbb{Q}$. Find a linear change of variables that transforms this curve into a curve of the form $Y^2=X^3+aX+b$ for rational numbers a and b.

2. (6 points) Let E be the elliptic curve over the finite field $K=\mathbb{Z}/5\mathbb{Z}$ defined by the equation
$$y^2=x^3+x+1.$$
   (i) List all 9 elements of $E(K)$.
   (ii) What is the structure of the group $E(K)$, as a product of cyclic groups?

3. (8 points) Let E be an elliptic curve over $\mathbb{Q}$. Define a binary operation $\boxplus$ on E as follows:
$$P \boxplus Q = -(P+Q).$$
   Thus the $\boxplus$ of P and Q is the third point of intersection of the line through P and Q with E.
   (i) Lists the axiom(s) of a group that fail for $E(\mathbb{R})$ equipped with this binary operation. (The group axioms are "identity", "inverses", and "associativity".)
   (ii) Under what conditions on $E(\mathbb{Q})$ does this binary operation define a group structure on $E(\mathbb{Q})$? (E.g., when $E(\mathbb{Q})=\{\mathcal{O}\}$ this binary operation does define a group.)

4. (6 points) 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.
   (i) Prove that the equations
$$x=\frac{\beta}{t-\alpha}, \qquad y=x^2u=\frac{\beta^2 u}{(t-\alpha)^2}$$
   give an "algebraic transformation" between the curve $u^2=g(t)$ and the curve $y^2=f(x)$, where $f(x)$ is the cubic polynomial
$$f(x)=g'(\alpha)\beta x^3+\frac{1}{2}g''(\alpha)\beta^2x^2+\frac{1}{6}g'''(\alpha)\beta^3x+\frac{1}{24}g''''(\alpha)\beta^4.$$
   (ii) Prove that if g has distinct (complex) roots, then f also has distinct roots, and so $u^2=g(t)$ is an elliptic curve.

5. (8 points) In this problem you will finally find out exactly why elliptic curves are called "elliptic curves"! Let $0 < \beta \leq \alpha$, and let C be the ellipse

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

(i) 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.

(ii) 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.

(iii) Prove that the integral in (i) is also equal to

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

(iv) Prove that if the ellipse E is not a circle, then the equation

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

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

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

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

6. (8 points) Suppose that $P = (x, y)$ is a point on the cubic curve

$$y^2 = x^3 + ax + b.$$

(i) Verify that the x coordinate of the point $2P$ is given by the duplication formula

$$x(2P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4y^2}.$$

(ii) Derive a similar formula for the y coordinate of $2P$ in terms of x and y.

(iii) Find a polynomial in x whose roots are the x-coordinates of the points $P = (x, y)$ satisfying $3P = \mathcal{O}$. [Hint: The relation $3P = \mathcal{O}$ can also be written $2P = -P$.]

(iv) For the particular curve $y^2 = x^3 + 1$, solve the equation in (iii) to find all of the points satisfying $3P = \mathcal{O}$. Note that you will have to use complex numbers.