Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 8

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, December 15th, at 12:05 pm.

1. The point $P = (3, 5)$ lies on the elliptic curve $E = E(\mathbb{Q})$ given by $y^2 = x^3 - 2$. Find a point on E with rational, non-integral coordinates. Do not forget to check that your calculations are correct!

2. Show that the sum of three points lying on an elliptic curve $E(\mathbb{R})$ is equal to $\mathcal{O}$, the common point of all vertical lines, if and only if the points are collinear (i.e., all lie on a single straight line).

3. Let a cubic be given by the following equation:

$$u^3 + v^3 = 1. \tag{1}$$

Find a birational transformation

$$\begin{aligned} x &= x(u, v) \\ y &= y(u, v) \end{aligned} \tag{2}$$

that transforms the curve (1) to a cubic in Weierstrass normal form:

$$y^2 = x^3 + bx + c,$$

where b and c are integers. Show that your transformation (2) is indeed birational.

4. Describe the projective plane over $\mathbb{F}_2$ using the standard construction via homogeneous coordinates. This plane is denoted by PG(2,2). You must present

(a) all points of PG(2,2) by giving their homogeneous coordinates;

(b) all “lines” in PG(2,2) as subsets of points from (a).

Hint. Each pair of points defines a line. Think which other points can belong to the same line.