Fachbereich Mathematik und Statistik
Dr. Michele Serra
Prof. Dr. Salma Kuhlmann
SS 2023

Introduction to Elliptic Curves

Exercise Sheet 1
Rational points

Exercise 1 **(2 points)**

Prove that the rational points on a line $L : aX + bY + cZ$ defined over $\mathbb{Q}$ are parametrised by $\mathbb{Q}$, i.e., they are in 1:1 correspondence with the rational numbers.

Exercise 2 **(2+2+2 points)**

We saw that the complex unit circle $X^2 + Y^2 + 1 = 0$ has no rational point. Here we show that the same holds for the circle $X^2 + Y^2 - 3 = 0$.

(a) Assume there is a rational point $\left(\frac{m}{n}, \frac{r}{s}\right)$ where the two fractions are reduced. Show that $n = s$.

(b) Show that, for all $x \in \mathbb{Z}$ we have $x^2 \equiv 0$ or $1 \pmod 3$.

(c) Deduce a contradiction to the reducedness of the fractions $\left(\frac{m}{n}, \frac{r}{s}\right)$.

Exercise 3 **(1+3 points)**

(a) Find a line in $\mathbb{A}^2(\bar{\mathbb{Q}})$ with no rational points.

(b) Find all the rational points of the conic (given in affine form by) $C : X^2 - 2Y^2 = 1$.

Exercise 4 **(2+2 points)**

(a) Show that the equation
$$X^4 + Y^4 = Z^2$$
has no integer solution (i.e. $x, y, z \in \mathbb{Z}$ such that $x^4 + y^4 = z^2$) with $(x, y) \neq (0, 0)$.

(b) Find all the rational points of the 4-Fermat curve
$$F_4 : X^4 + Y^4 = 1.$$

Please hand in your solutions by ***Wednesday, 3 May 2023, 13:30h*** *in the* ***postbox by F409*** *or per e-mail to your tutor.*