Elliptic curves: homework 1
Due: 12th February 2019, 14:00
Mastermath / DIAMANT, Spring 2019
Martin Bright and Marco Streng

Students are expected to (try to) solve all problems below, except possibly those marked as optional. The problems and their solutions are part of the course, and could play a role in the exam. More importantly, they help you digest the material of the previous lecture and/or help you prepare for the next lecture. Parts (b) and (c) of Exercises 2, 3, and 6 are to be handed in and count towards your grade.

Exercise 1 (optional)**.** Find a parametrization of the rational points on the circle over $\mathbb{Q}$ defined by the equation

$$x^2 + y^2 = 2.$$

Exercise 2 (hand in b and c)**.** Let C be the curve over $\mathbb{Q}$ in $\mathbb{A}^2$ given by the equation

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

(a) (optional) Show that $(0, 0)$ is the only point of C that is singular.

(b) Show that for every $\lambda \in \mathbb{Q}$, the line $y = \lambda x$ through the origin intersects C in exactly one other point $P_\lambda \neq (0, 0)$.

(c) Find a parametrization of the rational points on C.

Exercise 3 (hand in (b) and (c))**.** Let k be a field, $f \in k[X]$ a polynomial and $c \in \overline{k}$ an element of the algebraic closure of k.

(a) Show that we have $f(c) = f'(c) = 0$ if and only if there is a $g \in \overline{k}[X]$ with $f = (X - c)^2 \cdot g$. In this case, we call c a *multiple root* of f. If f has no multiple roots in $\overline{k}$, then we call f *separable.*

Suppose k has characteristic different from 2. Let C be the affine plane curve given by $Y^2 = f(X)$.

(b) Show that C is smooth if and only if f is *separable.*

(c) Take $f = x^3 + ax + b$ with $a, b \in k$. Show that C is smooth if and only if we have $4a^3 + 27b^2 \neq 0$.

Exercise 4. A commutative ring R with exactly one maximal ideal is called a *local ring.* Show that a commutative ring R is local if and only if $R \setminus R^*$ is an ideal of R.

Exercise 5 Let R be an integral domain with field of fractions K and $M \subset R$ a maximal ideal. Let

$$R_M = \left\{ \frac{a}{b} \in K : a \in R, b \in R \setminus M \right\}.$$

Show that R_M is a local ring. What is its maximal ideal?

Exercise 6 (hand in b and c)**.** A *discrete valuation* on a field K is a surjective group homomorphism $v : K^* \to \mathbb{Z}$ satisfying

$$v(x+y) \geq \min\{v(x), v(y)\}$$

for $y \neq -x$. The corresponding *discrete valuation ring* (DVR) is defined by

$$R_v = \{0\} \cup \{x \in K^* : v(x) \geq 0\}$$

(a) Show that for every prime number p the ring $\mathbb{Z}_{(p)}$ as in Exercise 5 is a DVR.

(b) Show that a discrete valuation ring R_v is a local ring, and that every element $\pi \in R_v$ with $v(\pi) = 1$ generates the maximal ideal of R_v. We call π a *uniformizer*.

(c) Let π be a uniformizer of a DVR R_v. Show that every non-zero ideal of R_v is of the form (π^i) for some $i \in \mathbb{Z}_{\geq 0}$.

Exercise 7. Let $V \subset \mathbb{A}^n$ be a variety defined by equations $f_1 = f_2 = \cdots f_m = 0$ with $f_i \in k[\vec{X}]$, and let $P \in V(\overline{k})$ be a point. Let M be the $m \times n$ matrix

$$M = \left(\frac{\partial f_i}{\partial X_j}(P) \right)_{ij}.$$

The *tangent space of V at P* is

$$P + \ker(M) = \{x \in \overline{k}^n \ : \ M(x - P) = \vec{0}\}.$$

(a) Find all vertical tangent lines of the curve C of Exercise 2.

(a) Find all horizontal tangent lines of the curve C of Exercise 2.