Elliptic curves: homework 1
Due: 22th September 2015, 10:15
Mastermath / DIAMANT, Fall 2015
Martin Bright and Marco Streng

Students are expected to (try to) solve all problems below. The first three problems are to be handed in and count towards your grade according to the rules on the web page. Problems marked with * are a bit harder than the average problem, you may want to postpone solving them until you have solved the other problems.

Homework to be handed in.

Exercise 1 For an integer $n > 0$, let C_n be the circle in the Euclidean plane defined by the equation

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

Find a parametrization of the rational points on the circle C_2.

Exercise 2 Let $F \in \mathbb{C}[x, y]$ be a non-constant polynomial, and C be the curve in $\mathbb{A}^2(\mathbb{C})$ defined by the equation

$$F(x, y) = 0.$$

A point (a, b) on C is said to be *singular* if we have

$$\frac{dF}{dx}(a, b) = \frac{dF}{dy}(a, b) = 0,$$

and *non-singular* or *smooth* otherwise.

(a) Suppose F is irreducible in $\mathbb{C}[x, y]$. Show that C has only finitely many singular points. (Hint: see Proposition 2 in Section 1.6 of [Fulton])

(b) Take $F = y^2 - f(x)$, with $f \in \mathbb{C}[x]$ a non-constant polynomial. Show that all points of C are smooth if and only if f is *separable*, i.e., without multiple roots.

(c) Take $f = x^3 + ax + b$ in (b). Show that all points of C are smooth if and only if we have $4a^3 + 27b^2 \neq 0$.

Exercise 3 Let C be the curve in $\mathbb{A}^2(\mathbb{C})$ given by the equation

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

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

(b) Show that every line $y = \lambda x$ through the origin intersects C in at most one other point $P_\lambda \neq (0, 0)$.

(c) Parametrize the rational points on C.

Additional homework, not to be handed in.

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 p be a prime number and let $R_p \subset \mathbb{Q}$ be the set of fractions $\frac{m}{n}$ with $p \nmid n$. Show that $R_p \subseteq \mathbb{Q}$ is a local ring.

Exercise 6 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 function $\mathrm{ord}_p : \mathbb{Q}^* \to \mathbb{Z}$ is a discrete valuation on $\mathbb{Q}$, and that the subring $R_p \subseteq \mathbb{Q}$ from the previous exercise is its corresponding discrete valuation ring.

(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.

*(c) Let π be as in (b). Show that every ideal of the DVR R_v is of the form (π^i) for some $i \in \mathbb{Z}_{\geq 0}$.

*(d) Show that a ring is a DVR if and only if it is a local principal ideal domain (PID) such that every ideal is a power of the maximal ideal.

Exercise 7

(a) Show that for any affine algebraic set V and any point P on V, the ring

$$O_P(V) = \{f/g \in k(V) : f, g \in \Gamma(V), g(P) \neq 0\}$$

is a local ring and find its maximal ideal.

*(b) Find an example where the ring $O_P(V)$ is a DVR and an example where it is not a DVR.

Exercise 8 Verify (1) – (10) in Sections 1.2 and 1.3 of [Fulton] and conclude that the maps I and V indeed give an inclusion-reversing bijection

$$\{\text{algebraic subsets of } \mathbb{A}^n(k)\} \longleftrightarrow \{\text{ideals of algebraic subsets of } \mathbb{A}^n(k)\}.$$

Hint for (7): do Problems 1.4 and 1.7 of [Fulton].

Exercise 9 [Fulton] Problem 1.25.