Elliptic curves: exercise sheet 1

Due: 17th September 2013

Mastermath / DIAMANT, Fall 2013

René Schoof and Peter Stevenhagen

Exercise 1. Let (a, b, c) be a *Pythagorean triple*, i.e., a triple (a, b, c) of positive integers satisfying $\gcd(a, b, c) = 1$ and

$$a^2 + b^2 = c^2.$$

Show that, possibly after interchanging a and b, there exist integers $m > n > 0$ such that we have

$$a = m^2 - n^2, \qquad b = 2mn, \qquad c = m^2 + n^2.$$

Exercise 2. For an integer $n > 0$, let C_n be the circle in the Euclidean plane defined by the equation

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

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

(b) Determine for which primes p there exist rational points on C_p.

(c) Can you extend the result of (b) to the case of arbitrary integers n?

Exercise 3. Consider the difference $19 = 3^3 - 2^3$ of rational cubes.

(a) Write 19 as a *sum* of two positive rational cubes.

(b) Is the solution in (a) unique?

*(c) Is the number of rational solutions to the equation $x^3 + y^3 = 19$ finite or infinite?

Exercise 4. State and prove the Porism of Diophantus (on differences of cubes being sums of cubes) in full generality.

Exercise 5. Let $E_k : U^3 + V^3 = kW^3$ be the 'porism curve', written in projective coordinates U, V and W. Find a linear change of coordinates $(U, V, W) \to (X, Y, Z)$ with rational coefficients that transforms E_k into a Weierstrass curve $Y^2Z = X^3 + AXZ^2 + BZ^3$, and compute A and B.

Exercise 6. Let $F \in \mathbf{C}[x, y]$ be a non-constant polynomial, and C be the curve in $\mathbf{C}^2$ defined by the equation

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

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

$$\frac{\mathrm{d}F}{\mathrm{d}x}(a, b) = \frac{\mathrm{d}F}{\mathrm{d}y}(a, b) = 0,$$

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

(a) Suppose F is irreducible in $\mathbf{C}[x, y]$. Show that C has only finitely many singular points.

(b) Take $F = y^2 - f(x)$, with $f \in \mathbf{C}[x]$ 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 7. Let C be the cubic curve in $\mathbf{C}^2$ 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) Can you parametrize the rational points on C?

Exercise 8. Let $\mathbf{F}_q$ be a finite field with q elements. The zeta function of the ring $R = \mathbf{F}_q[X]$ is defined by

$$\zeta_R(s) = \sum_{I \subset R} \frac{1}{[R : I]^s}, \qquad \text{for } s \in \mathbf{C} \text{ with } \operatorname{Re} s > 1.$$

Here I runs over the non-zero ideals of R.

(a) Show that

$$\zeta_R(s) = \prod_{d=1}^{\infty} \left(\frac{1}{1 - q^{-ds}} \right)^{a_d},$$

where a_d denotes the number of monic irreducible polynomials of degree d in R.

(b) Determine a_d for $1 \leq d \leq 6$.

Exercise 9. Let p be a prime and let C be the curve in $\mathbf{A}^2$ given by $X^2 + Y^2 + 1 = 0$.

(a) Determine the cardinalities of the subsets $\{x^2 + 1 : x \in \mathbf{F}_p\}$ and $\{-y^2 : y \in \mathbf{F}_p\}$ of $\mathbf{F}_p$.

(b) Show that C has a point with coordinates in $\mathbf{F}_p$.

(c) Determine the number of points of C with coordinates in $\mathbf{F}_p$.

Exercise 10. Hilbert's Nullstellensatz says that if k is a field and A is a finitely generated k-algebra that is also a field, then A is a finite extension of k.

(a) Use the Nullstellensatz to prove that if k is algebraically closed, then the maximal ideals of the ring $k[X_1, \ldots, X_n]$ are of the form $(X_1 - a_1, \ldots, X_n - a_n)$ for certain $a_1, \ldots, a_n \in k$.

*(b) Use the Nullstellensatz to prove that for every maximal ideal $\mathfrak{m}$ of $\mathbf{Z}[X_1, \ldots, X_n]$ the residue field $\mathbf{Z}[X_1, \ldots, X_n]/\mathfrak{m}$ is finite.