**Mastermath course "Elliptic curves" - exercise set 1**

1. For an integer $n > 0$, let $C_n$ be the circle in the Euclidean plane defined by the equation
$$x^2 + y^2 = n.$$
   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 $n$?

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

3. Consider the difference $19 = 3^3 - 2^3$ of rational cubes.
   a. Write 19 as a *sum* of two positive rational cubes.
   b. Can you find different solutions to a?
   *c. Is the number of different solutions to a finite or infinite?

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

5. Let $\phi : \mathbf{C} \to \mathbf{C}^2$ be the map defined by $z \mapsto (\sin z, \cos z)$.
   a. Show that the image of $\phi$ is the algebraic set
$$S = \left\{(x, y) \in \mathbf{C}^2 : x^2 + y^2 = 1\right\}.$$
   b. Show that $\phi$ induces a bijection between the elements of the quotient *group* $G = \mathbf{C}/2\pi\mathbf{Z}$ and $S$.
   c. Show that the "natural" addition of points $(x, y) \in S$ induced by $\phi$ is given by an algebraic formula, and find this formula.
   d. How many points $P \in S$ satisfy $2011 \cdot P = (0, 1)$?

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 $4a^3 + 27b^2 \neq 0$.

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 $C$?