EXERCISES FOR TUTORIAL 2

These exercises were already suggested in Tutorial 1, we will discuss the answers during Tutorial 2.

Exercises

- 2.2 and 2.3 with SageMath
- 2.9 is the general addition law with
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$
it can be done with SageMath.

Moreover we will do:

- 2.4 with SageMath
- 2.5
- 2.6
- 2.8 with the algorithm of the book (least significant bits first) then with the variant in the slides of Lecture 2 (most-significant bits first)
- 2.7 with SageMath
- using the file `curve_arithmetic.py`, write the double-and-add algorithm of the book page 18 (integer-times-a-point), and the Most-Significant-Bits First version of the lecture (slides of Lecture 02).
  - With the short Weierstrass equation and the affine formulas, check with what would answer SageMath
  - With the Edwards form and the affine Edwards formula: this is too long, it is only optional.
- Points of order 2: Given an elliptic curve
$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$
over a field $\mathbb{K}$, what are the points of order 2 in terms of their coordinates (x, y)? Hint: it means that the tangent at P of order 2 is a vertical. What do you deduce about the factorisation of $f(x) = x^3 + a_2x^2 + a_4x + a_6$ and the coordinates (x, y)? If $x_0 = 0$ is a root of $f(x)$, which conditions on the coefficients a_i ensure to have as many points of order 2 as possible?
- Points of order 3: these are inflexion points. What are the conditions on the a_i to get points of order 3, and what are their coordinates (x, y) in terms of roots of an appropriate polynomial?

Date: Week 2.