Homeworks: Algorithms on Elliptic Curves

2024/25

There will be four homework assignments for which a maximum of 40 points can be obtained in total. A minimum of 25 points is required for credit.

All steps should be explained in detail (preferably by references to assertions, examples, or exercises).

1. Homework

To be submitted till 2nd April, 2 pm

1.1. Find a short WEP which is $\mathbb{F}_7$-equivalent to the WEP

$$w = y^2 + y(2x+1) - (x^3 + 2x^2 + 2x - 1) \in \mathbb{F}_7[x, y].$$

5 points

1.2. Decide whether the WEP is $y^2 - (x^3 + 4x^2 - x - 4) \in K[x, y]$ is smooth if
(a) $K = \mathbb{Q}$, (b) $K = \mathbb{F}_5$.

5 points