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 26th March, 2 pm

1.1. Find a short WEP which is $\mathbb{F}_3$-equivalent to the WEP

$$w = y^2 + y(2x+1) - (x^3 + 2x^2 + 2x) \in \mathbb{F}_3[x, y].$$

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

2. Homework

To be submitted till 30th April, 2 pm

2.1. Find all elements and draw the tables of the group operations $\ominus$, $\oplus$ of the group of the elliptic curve C given by the WEP $w = y^2 - (x^3 + x) \in \mathbb{F}_5[x, y]$.

4 points

2.2. Decide whether the WEP $y^2 - (x^3 + 3x - 1) \in \mathbb{F}_7[x, y]$ is $\mathbb{F}_7$-equivalent to some Montgomery polynomial.

3 points

2.3. Depending on the binary length $k = l_2(n)$ and the number of inversions, multiplications and squarings (I, M, S) in a field $\mathbb{F}$, estimate the time complexity of computing the power $[n]P$ of an element P of the Montgomery curve using the Montgomery's ladder.

3 points

3. Homework

To be submitted till 14th May, 2 pm

3.1. Find a polynomial $f \in \mathbb{F}_5[x, y]$ such that V_f is an Edwards curve which is birationally equivalent to the curve Montgomery curve V_m over $\mathbb{F}_5$ if (a) $m = 2y^2 - (x^3 + x^2 + x)$, (b) $m = y^2 - (x^3 - x^2 + x)$.

3 points

3.2. Find a polynomial $m \in \mathbb{F}_5[x,y]$ such that V_m is a Montgomery curve which is birationally equivalent to the curve Edwards curve $V_{y^2+x^2-(1+2x^2y^2)}$ over $\mathbb{F}_5$. Find the point of V_m corresponding to the point $(2,2)$ of $V_{y^2+x^2-(1+2x^2y^2)}$.

2 points

3.3. Let K be a field, $s,t,r \in \overline{K}$ such that $s^2 = d$, $t^2 = \frac{d}{a}$, $r^2 = a^{-1}$,

$$\hat{F}(X_1,X_2,Y_1,Y_2) = X_2^2Y_1^2 + aX_1^2Y_2^2 - (X_2^2Y_2^2 + dX_1^2Y_1^2) \in K[X_1,X_2,Y_1,Y_2],$$

and $f = \hat{F}(x,1,y,1)$. If $\sigma_\pm = ((1:\pm s),(1:0))$ and $\tau_\pm = ((1:0),(1:\pm t))$, put

$$H = \{\nu(0,1), \nu(0,-1), \nu(\pm r, 0), \sigma_\pm, \tau_\pm\}.$$

Prove that H is a subgroup of $(\hat{V}_{\hat{F}}, \oplus, \ominus, \nu(0,1))$ and explicitly describe an isomorphism $\mathbb{Z}_4 \times \mathbb{Z}_2$. How many such isomorphisms exists?

(You can use all claims of the Exercise 4.8)

5 points