Algorithms on Elliptic Curves, exam, sample, 2025

Formulate claims and definitions including all assumptions. Explain your statements or computations briefly.

You can earn 2 points for each task.

(1) Define a functional field of an affine curve.
(2) Write a non-trivial example of a discrete valuation of a functional field.
(3) Decide whether the WEP $y^2 - (x+1)(x+2)(x+4)$ is smooth over$\mathbb{F}_{13}$.
(4) Describe all elements of the exponent 2 of a smooth affine Weierstrass curve V_{y^2-f}.
(5) For the Montgomery curve $V_{2y^2-(x^3+3x^2+x)}$ over a field $\mathbb{F}_7$ find a $\mathbb{F}_7$-equivalent affine Weierstrass curve.
(6) What is a Montgomery's ladder?
(7) What does it mean that two curves are birationally equivalent?
(8) Describe all singularities of a twisted Edwards curve.
(9) If the characteristic of a finite field is p and $\gcd(p, m) = 1$, describe the structure up to isomorphism of the subgroup of m-torsion elements $E[m]$ of a group E of an elliptic curve.
(10) Define the polynomials $\tilde{\Psi}$.