Algorithms on Elliptic Curves

1. List of questions for the short test

1.1. **Curves and functional fields.**

1. Define an irreducible affine curve.

2. Define an irreducible projective curve.

3. Define a functional field of an affine curve.

4. What does it mean that a curve/polynomial is smooth?

5. Define smoothness and singularity of a general affine (or projective) curve.

6. Write a non-trivial example of a discrete valuation of a functional field.

7. Decide whether the affine curve V_{y-x^2} (or $V_{y^2+x^2}$, $V_{y^2-x^2}$, $V_{(y-x)^5}$ etc.) over $\mathbf{R}$ (or $\mathbb{C}$) is irreducible.

1.2. **Weierstrass curves.**

8. Define a general (or short) Weierstrass curve.

9. What is an affine map and an affine homomorphism/transformation?

10. Define K-equivalence of Weierstrass curves over a field K.

11. Decide whether the WEP $y^2-(x+1)(x+2)(x+4)$ (or $y^2-(x^3+4x+2)$ etc.) is smooth over $\mathbb{F}_5$ (or $\mathbb{F}_7$, $\mathbb{F}_{11}$ etc.).

12. Find all singularities of the curve $V_{y^2-(x+1)(x+2)(x+4)}$) (or $V_{y^2-(x-1)^3}$ etc.) over $\mathbb{F}_5$ (or another field).

1.3. **Arithmetic on a Weierstrass curve.**

13. Describe the group structure on a smooth affine Weierstrass curve $V_{y^2-(x^3+ax+b)}$ (either by formulas or by geometrical view).

14. Describe all elements of the exponent (order) 2 of a smooth affine Weierstrass curve V_{y^2-f}.

1.4. **Montgomery curves.**

15. Define a Montgomery curve.

16. For a Montgomery curve $V_{By^2-(x^3+Ax^2+x)}$ over a field K describe a K-equivalent affine Weierstrass curve.

17. 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.

18. How does relate the group structure of a Montgomery curve and of the corresponding Weierstrass curve?

19. What is a Montgomery's ladder?

20. Calculate the Montgomery's ladder for $n=23$ (or another small n).

1.5. **Edwards curves.**

21. Define an Edwards curve and a twisted Edwards curve.

22. What does it mean that two curves are birationally equivalent?

23. Describe all singularities of a twisted Edwards curve.

24. What are completed coordinates of a twisted Edwards curve?

25. For the Montgomery curve given by $3y^2 - (x^3 + 3x^2 + x) \in \mathbb{F}_7[x, y]$ find a birationally equivalent twisted Edwards curve.

26. For the twisted Edwards curve given by $2x^2 + y^2 - 1 + 3x^2y^2 \in \mathbb{F}_7[x, y]$ compute a birationally equivalent Montgomery curve.

1.6. **Torsion subgroups of an elliptic curve.**

27. How many involutions contains any group of an elliptic curve over a finite field of the characteristic > 3?

28. 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 $E[m]$ (or p^e-torsion elements) of a group E of an elliptic curve.

29. Formulate the Hasse theorem on the cardinality of the subgroup of $\mathbb{F}_q$-rational elements of a group of an elliptic curve over $\mathbb{F}_q$.

1.7. **Schoof's algorithm.**

30. Define the polynomials $\tilde{\Psi}_n$.

31. Define the endomorphism φ on a projective elliptic curve. How does it act on a projective elliptic curve?

32. Formulate the assertion about relations of φ^2, φ and id in $\mathbb{Z}$-algebra of the endomorphisms of an elliptic curve.

2. Theoretical questions for the discussion

1. Explain the role of smooth Weierstrass curves in the theory of elliptic curves. Formulate and prove two equivalent condition for a Weierstrass curve to be smooth (2.2, 2.3).

2. Explain the relationship between smooth Weierstrass curves and Montgomery curves. Describe the algorithm of computing powers $[n]P$ using Montgomery's ladder.

3. Explain the relationship between smooth Weierstrass curves and Montgomery curves. Describe which Weierstrass curves can be represent as Montgomery curves and prove your claim (4.5, 4.6).

4. Prove that every twisted Edwards curve is irreducible (5.1, 5.2) and explain the correspondence between twisted Edwards and Weierstrass curves.

5. Describe and prove the description of the correspondence between twisted Edwards and Montgomery curves (5.8).

6. Explain the Schoof's algorithm.