2007 - Exercises VIII.

1. Consider the elliptic curve $y^2 = x^3 + x + 6$ over the field $\mathbb{F}_{11}$.
   (a) Determine the number of multiple roots of this elliptic curve.
   (b) Compute in detail the points $(2,7) + (5,2)$ and $(3,6) + (3,6)$.

2. Let E be the elliptic curve $y^2 = x^3 + 2$ over the field $\mathbb{F}_7$.
   (a) Find the points of E.
   (b) Which group is the elliptic curve E isomorphic to?

3. Let $y^2 = x^3 + 9x + 17$ be the elliptic curve over the field $\mathbb{F}_{23}$. What is the discrete logarithm k of $Q = (4,5)$ to the base $P = (16,5)$?

4. Consider the following elliptic curve cryptosystem.

   An elliptic curve $E : y^2 = x^3 + ax + b$ over the field $\mathbb{Z}_p$ and a generator point $G \in E$ of order n are public parameters.

   Each user U selects as a private key a number $s_U < n$ and computes the corresponding public key $P_U = s_U G$.

   To encrypt a message point M, one selects a random k and computes the ciphertext pair of points $C = [(kG), (M + kP_U)]$.

   (a) Show how the user U can decrypt C and obtain M.
   (b) Let E be $y^2 = x^3 + x + 6 \pmod{11}$, $G = (2,7)$ and $s_A = 7$.
   Recover the plaintext message point M from $C = [(8,3), (10,2)]$.

5. Factorize $n = 4453$ using the elliptic curve $y^2 = x^3 + 10x - 2 \pmod{n}$ and the point $P = (1,3)$.

6. (a) Factorize the following numbers $n_1 = 527$ and $n_2 = 1241$ using the Pollard's ρ-algorithm (the first one from the lecture) with $f(x) = x^2 + 1$ and $x_0 = 0$.
   (b) Factorize the following numbers $n_1 = 65$ $(b = 10)$ and $n_2 = 15770708441$ $(b = 200)$ using the Pollard's $p - 1$ algorithm.

7. Consider the Pollard's ρ-algorithm with a pseudo-random function $f(x) = x^2 + c \pmod{n}$ with a randomly chosen c, $0 \leq c < n$. Why should be the values $c = 0$ and $c = n - 2$ avoided?

8. Show that $n^{13} - n$ is a multiple of 420 for any odd n.