*IV054 Coding, Cryptography and Cryptographic Protocols*
**2011 - Exercises VIII.**

1. Let $n \geq 2$ be an integer. Show that the number $n^{40} + 1$ is composite.
2. Does the elliptic curve equation $y^2 = x^3 + 10x + 5$ define a group over $\mathbb{F}_{17}$?
3. (a) Use the first Pollard's rho method with pseudorandom function $f(x) = x^2 + 1$ and $x_0 = 3$ to find a factor of 4577.
   (b) Find a factor of 143 using the curve $E : y^2 = x^3 + 2x + 1 \pmod{143}$ and its point $P = (1, 119)$.
4. To which group is the elliptic curve $E : y^2 = x^3 + 4x + 1$ over $\mathbb{Z}_7$ isomorphic to? Compute the addition table of $E$.
5. Find an integer $1 < x < 2011$ such that $x^{11} - 1$ is a multiple of 2011 or show that such an integer does not exist.
6. Design an elliptic curve counterpart of Shank's algorithm and answer the following questions.
   (a) In classical Shank's algorithm with modulus $p$, both parameters $i, j$ run in interval $0 \leq i, j < \lceil \sqrt{p-1} \rceil = m$. Why?
   (b) What is the bound for its elliptic curve counterpart – an elliptic curve $E \pmod{p}$ with the number of points $N > p + 1$?
   (c) Using the designed algorithm solve $(7, 9) = x(2, 7)$ for the elliptic curve $E : x^3 + x + 6 \pmod{11}$ and show the computed table.
7. *(Bonus)* Let $\mathbb{F}_{2^m}$ be a finite field with characteristic 2 and a generator $g$. Let $a, b \in \mathbb{F}_{2^m}$ satisfy $b \neq 0$. The field is described using the irreducible polynomial $x^3 + x + 1$. An elliptic curve over such field consists of the set of solutions $(x, y)$ for $x,\ y \in \mathbb{F}_{2^m}$ to the equation $y^2 + xy = x^3 + ax^2 + b$.
   Let $m = 3$ and $E : y^2 + xy = x^3 + g^2x^2 + g^6$ be an elliptic curve over this field.
   (a) Define negatives for elliptic curves over $\mathbb{F}_{2^m}$ in general and find $-(g^3, g^6)$ in $E$.
   (b) Define addition of two points with different $x$-coordinates for elliptic curves over $\mathbb{F}_{2^m}$ in general and find $(g^2, g^6) + (g^5, g^5)$ in $E$.
   (c) Define doubling of a point for elliptic curves over $\mathbb{F}_{2^m}$ in general and find $2 \cdot (g^3, g^4)$ in $E$.