IV054 Coding, Cryptography and Cryptographic Protocols
2017 - Exercises VIII.

1. Find all points lying on the elliptic curve $E: y^2 = x^3 + 3x + 5 \mod 7$.
2. Sign your UČO (Personal identification number) with the following algorithm:
   (a) Hash your UČO using a hash function $h(x) = 5^x \mod 1033$ and label the result h.
   (b) Sign h with an elliptic curve variant of the ElGamal signature scheme with
   $$E: y^2 = x^3 + 3x + 983 \mod 997,$$
   public points $P = (325, 345)$, $Q = aP = (879, 211)$ and secret key $a = 140$. Use random integer $r = 339$. Note that order of P in E is 1034.
3. (a) Using Pollard $(p-1)$-method find a factor of 1781. Use the fixed integer $B = 12$.
   (b) Using Pollard ρ-method (Version 1) with $x_i = x_{i-1}^2 + x_{i-1} + 1 \mod n$ and starting integer $x_0 = 15$ find a factor of 473.
4. Consider elliptic curves over a finite field $\mathbb{F}_5$.
   (a) Show that for every elliptic curve $E \mod 5$, we have $2 \leq |E| \leq 10$.
   (b) Give three elliptic curves over $\mathbb{F}_5$ with distinct numbers of points.
5. Find a factor of 119 without using brute force if you know that the function $29^x \mod 119$ has a period $r = 20$.
6. Consider elliptic version of the ElGamal cryptosystem. Public key is as follows:
   $p = 11$, $E: y^2 = x^3 + 3x + 6 \mod 11$, $P = (2, 8)$, $Q = (2, 3)$.
   Show computation steps.
   (a) Encrypt the message $m = (5, 6)$ with $r = 2$.
   (b) Decrypt the ciphertext, computed in (a), with private key $x = 4$.
7. Show that if the number of points of an elliptic curve E can be factorized into the product of distinct primes, then the group $(E, +)$ is cyclic.
8. Give an example of two elliptic curves with the same number of points but with a different group structure, which are both defined over
   (a) GF(3);
   (b) GF(5);
   (c) GF(7).