IV054 Coding, Cryptography and Cryptographic Protocols
2019 - Exercises VIII.

1. *(3 points)*
   (a) How many points are there on the elliptic curve $E: y^2 = x^3 + 5x + 4$ over $\mathbb{F}_{11}$?
   (b) What is the order of point $P = (10, 3)$?
   (c) How can we easily say that some point on E has order 2?

2. *(3 points)*
   (a) Use Pollard's ρ-method (both version 1 and version 2) to factorize 3551, starting with $x_0 = 2$ and using pseudo-radom function $x_{i+1} = x_i^2 + 3 \pmod{3551}$.
   (b) Use Pollard's $p-1$ method to factorize 178297. Use $B = 23$, $a = 2$.

3. *(3 points)* Sign your UČO 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 $P = (325, 345), Q = xP = (879, 211)$ and secret key $x = 140$. Use random component $r = 339$. Note that order of P in E is 1034.

4. *(4 points)* Find two elliptic curves over $\mathbb{F}_5$ with 8 points but with a different group structure.

5. *(2 points)* Consider an elliptic curve $E : y^2 = x^3 + 8$ over $\mathbb{R}$. Show that E does not have multiple roots. Algebraically determine the number of roots E has.

6. *(4 points)* Is there a non-singular elliptic curve over $\mathbb{Z}_{11}$ having:
   (a) 5 points;
   (b) 6 points;
   (c) 14 points;
   (d) 19 points.

   all including the point in infinity $\mathcal{O}$. If there exists such curve, find it and list its points. Otherwise, prove that such an elliptic curve cannot exist.

7. *(3 points)* Show that $42 \mid n^7 - n$ for all integers $n \in \mathbb{N}$.

8. *(4 points)* Recall the definition of a Fermat number:

   $$F_n = 2^{2^n} + 1$$

   where n is a non-negative integer. Prove the following claims:
   (a) For $n \geq 1$, $F_n = F_0 \cdots F_{n-1} + 2$.
   (b) For $n \geq 2$, the last digit of F_n is 7.
   (c) No Fermat number is a perfect square.
   (d) Every Fermat number F_n for $n \geq 1$ has the form $6m - 1$ for an integer $m > 0$.

9. *(4 points)* Consider the following cryptosystem using a non-singular elliptic curve E_p for a prime p with n points, secret key $d < n$ and public key (P, Q), where P, Q are two points on E_p with $Q = dP$.

   To encrypt a message $m = (m_1, m_2)$, $1 \leq m_1, m_2 < p$, pick a random integer $1 \leq k < n$ and compute $R = kP$, $y_1 = c_1 m_1 \mod p$ and $y_2 = c_2 m_2 \mod p$ where $(c_1, c_2) = kQ$.
   The encrypted message is then (R, y_1, y_2).

   Find and describe the decryption procedure.