IV054 Coding, Cryptography and Cryptographic Protocols
2020 - Exercises VIII.

1. *(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 it 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 the order of P in E is 1034.

2. Consider elliptic curves over $\mathbb{F}_7$.
   (a) *(3 points)* Give examples of an elliptic curve with the minimal and with the maximal number of points. List their points. Justify your answer.
   (b) *(5 points)* Give an example of two elliptic curves having 9 elements but with a different group structure. Justify your answer.

3. *(5 points)* Let $E_p : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{F}_p$ where p is a prime.
   (a) Prove the following theorem:
   $$|E_p| = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p} \right)$$
   where $\left(\frac{x}{p}\right)$ is the Legendre symbol.
   (b) Give an upper bound on $\left| \sum_{x=0}^{p-1} \left(\frac{x^3+ax+b}{p} \right) \right|$.

4. *(3 points)* Using the fact that the function $f(x) = 2^x \mod 1927$ has a period $r = 460$, factorize 1927 without using brute force.

5. *(3 points)* Consider the elliptic curve $E : y^2 = x^3 + 3x + 7 \pmod{113}$ with points $(74, 3)$ and $(28, 11)$ having order 3 and 14, respectively.

   Calculate the number of points of E. (Do not use brute force.)

6. *(3 points)* Alice and Bob are using the elliptic curve variant of the Diffie-Hellman key exchange protocol. You managed to intercept Alice sending $n_A P = (55, 0)$ to Bob but nothing else, not even the public elliptic curve they are using. What are all the possible keys Alice and Bob can now share?