IV054 Coding, Cryptography and Cryptographic Protocols
2018 - Exercises VIII.

1. Consider the elliptic curve $E : y^2 = x^3 + 3x + 5$ over the field $\mathbb{F}_7$.
   (a) Find all points of E.
   (b) Compute in detail $15P$ where $P = (1, 3)$.
2. Sign your UČO with the following algorithm:
   i Hash your UČO using a hash function $h(x) = 5^x \mod 1033$ and label it h.
   ii 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 $r = 339$. Note that order of P in E is 1034.
3. (a) Use the Pollard ρ-factorization method (Version 1) with $x_i = x_{i-1}^2 + x_{i-1} + 1 \pmod n$ and $x_0 = 446$ to factorize $n = 10229$.
   (b) Use the Pollard ρ-factorization method (Version 2) with $x_i = x_{i-1}^2 + 1 \pmod n$ and $x_0 = 5$ to find a factor of $n = 21583$.
   (c) Use the Pollard $p - 1$ method with $B = 11$ and $a = 2$ to find a factor of 198299.
   (d) Use the Quadratic sieve method to factorize $n = 713$.
4. Give an example of an elliptic curve
   (a) over the finite field $\mathbb{F}_5$;
   (b) with exactly one point;
   (c) with q points over a finite field $\mathbb{F}_q$;
   (d) over the finite field $\mathbb{F}_2$.
5. Give an example of two elliptic curves defined over $\mathbb{F}_{11}$ such that they have the same number of elements but a different group structure.
6. Describe a three-pass protocol[1] using elliptic curves such that an adversary eavesdropping on the communication would have to solve the Diffie-Hellman problem to decrypt the sent message.
7. Find all points of the elliptic curve $E : y^2 + xy = x^3 + 1$ over the field $\mathbb{F}_4$.

[1] `https://en.wikipedia.org/wiki/Three-pass_protocol`