IV054 Coding, Cryptography and Cryptographic Protocols
2015 - Exercises IX.

1. Consider the elliptic curve $E : y^2 = x^3 + 2x + 1 \pmod{11}$.
   (a) Find all points of the curve E.
   (b) Solve $x(0, 1) = (5, 9)$ for x.
2. Consider elliptic curves over $\mathbb{Z}_5$. Which group are the following elliptic curves isomorphic to?
   (a) $y^2 = x^3 + x + 1$
   (b) $y^2 = x^3 + 4x + 2$
   (c) $y^2 = x^3 + 4x + 3$
3. Use the first version of Pollard ρ-factorization with $x_0 = 15$ to factorize 39271.
4. Consider the elliptic curve variant of the Diffie-Hellman key exchange protocol with the eliptic curve $E : y^2 = x^3 + 3x + 4 \pmod{17}$ and the point $P = (1, 5)$. Let Alice's choice of integer be $n_a = 3$ and let Bob's choice be $n_b = 4$. Finish the protocol and show your steps.
5. Consider an elliptic curve version of the ElGamal signatures with public information $p = 13$, $E : y^2 = x^3 + 3x + 5 \pmod{13}$, $P = (1, 3)$, $Q = (11, 11)$ and private information $a = 4$.
   (a) Sign the message $m = 6$ with $r = 5$.
   (b) Verify the signature $(4, (12, 12), 5)$.
6. Let E be the elliptic curve over $\mathbb{Q}$ defined by the equation $y^2 = x^3 - 7x + 6$. Find all of its 2-torsion points, *eg.* points P such that $P = -P$.
7. Is there a (non-singular) elliptic curve E defined over $\mathbb{Z}_5$ such that
   (a) E contains exactly 11 points (including the point at infinity $\mathcal{O}$);
   (b) E contains exactly 10 points (including the point at infinity $\mathcal{O}$)?

   If the answer is positive, find such a curve and list all of its points, If it is negative, prove it.