IV054 Coding, Cryptography and Cryptographic Protocols
2016 - Exercises VIII.

1. Consider the elliptic curve $E : y^2 = x^3 + 3x + 5 \pmod 7$.
   (a) Let $P = (1, 3)$. Calculate $3P$.
   (b) List all the points on the elliptic curve E.
   (c) Find Q_1 such that $4Q_1 = P = (1, 3)$.
   (d) Find Q_2 such that $4Q_2 = \infty$.
2. Is there a (non-singular) elliptic curve E defined over $\mathbb{Z}_7$ such that
   (a) E contains exactly 12 points (including ∞)?
   (b) E contains exactly 14 points (including ∞)?

   In case of a positive answer, find such a curve and list all of its points. Otherwise, prove that such a curve does not exist.
3. Find all points of order 2, *ie.* points P such that $2P = \infty$, of the elliptic curve $E : y^2 = x^3 - x$ over $\mathbb{R}$.
4. Propose a simple method to compute mP on an elliptic curve with approximately $\log_2 m$ point doublings and $\frac{1}{2} \log_2 m$ or less additions on average.
5. (a) Using Pollard ρ-method find a factor of 2899 using the function $f(x) = 3x+13$ and the starting integer $x_0 = 7$.
   (b) Using Pollard $(p - 1)$-method find a factor of 37787 using the fixed integer $B = 10$.
6. Consider the elliptic curve version of the ElGamal digital signature from the lecture.
   (a) Show that the private key a can be recovered if an adversary learns r.
   (b) Show that the private key a can be recovered if the same r is used to generate signatures on two messages.
   (c) Let $E : y^2 = x^3 + x + 4 \pmod{23}$ and let $P = (0, 2)$. Show that an adversary can forge valid signature on any message of its choice. Propose a method to prevent such an attack.
7. Consider the elliptic curve
   $$E : y^2 = x^3 + 1 \pmod p,$$
   where p is a prime, $p \equiv 2 \pmod 3$ and $p \geq 5$. Find the number of points on such an elliptic curve and prove your answer.