IV054 Coding, Cryptography and Cryptographic Protocols
2014 - Exercises VIII.

1. Using the Rabin-Miller primality test with $a = 2$, decide whether $n = 294409$ is a prime.

2. Let n, x be integers and $n \geq 2$, $x \geq 1$. Show that the number $n^{10x} + 1$ is composite.

3. Let elliptic curve be $E : y^2 = x^3 - x \pmod 7$. Let $P_1 = (4, 2)$ and $P_2 = (5, 1)$, find $P_1 + P_2$, $2P_1$ and $3P_1$. List all the points on the elliptic curve.

4. Find a point P on the elliptic curve $E : y^2 = x^3 + 3x + 2 \pmod 5$, such that $P + P = (2, 4)$. Show details of your computation.

5. Design an elliptic curve counterpart of the Shanks' algorithm.
   (a) In classical Shanks' algorithm with modulus p, both parameters i, j run in interval $0 \leq i, j < \lceil\sqrt{p-1}\rceil = m$. Why?
   (b) What value of m should we set for its elliptic curve counterpart, with an elliptic curve $E \pmod p$ and its number of points N?
   (c) Using the designed algorithm solve $(7, 9) = x(2, 7)$ for x, given $E : y^2 = x^3 + x + 6 \pmod{11}$, and show the computed table.

6. Bob uses an elliptic curve version of the ElGamal cryptosystem with public key $p = 7$, $E : y^2 = x^3 + 3x + 5 \pmod 7$, $P = (1, 3)$, $Q = (6, 6)$.
   (a) Encrypt the message $m = (1, 4)$ with $r = 3$. Show computation steps.
   (b) Decrypt the ciphertext computed in (a) with Bob's secret key $x = 2$. Show computation steps.

7. (a) $P = (x, 0)$ is a point on an elliptic curve. Find nP, $n \in \mathbb{N}$.
   (b) Show that three different points on an elliptic curve add to ∞ if and only if they lie in a straight line.