IV054 Coding, Cryptography and Cryptographic Protocols
2012 - Exercises VIII.

1. Consider the elliptic curve $E : y^2 = x^3 + 3x^2 + 6x + 17$ over $\mathbb{Z}_{23}$.
   (a) Verify that the point $P = (2, 7)$ lies on E.
   (b) Using a transformation into the form $y^2 = x^3 + ax + b$ compute the point $2P$.

2. Consider the following primality test. An integer $n > 0$ is a prime if and only if n divides $2^n - 2$. Prove or disprove both implications.

3. Consider the elliptic curve
$$E = \{\mathcal{O}\} \cup \{(x, y) \in \mathbb{Z}_7^2 \mid y^2 = x^3 + 2x + 1\}.$$
   (a) Find all points of E. Compare the number of points with the Hasse's theorem.
   (b) For each point $P \in E$, compute $-P$ and check that it lies on the curve as well.
   (c) Show that $(E, +)$ is isomorphic to $\mathbb{Z}_{|E|}$.

4. Suppose $n = pq$, where p, q are primes. Let integers i, j, k and L with $k \neq 0$ satisfy
$$L = i(p-1), \quad L = j(q-1) + k \quad \text{and} \quad a^k \not\equiv 1 \pmod{q}.$$
   Let a be a randomly chosen integer satisfying $p \nmid a$ and $q \nmid a$. Prove that
$$\gcd(a^L - 1, n) = p.$$

5. (a) Use the ρ-algorithm with $f(x) = x^2 + 1$ and $x_0 = 2$ to find a factor of $n = 8383$.
   (b) Try to factorize $n = 551$ using the elliptic curve $E : y^2 = x^3 + 4x + 4$ and
      (i) point $P_1 = (1, 3)$,
      (ii) point $P_2 = (0, 2)$.

6. Prove the following theorems.
   (a) If n is even and $n > 2$, then $2^n - 1$ is composite.
   (b) If $3 \mid n$ and $n > 3$, then $2^n - 1$ is composite.
   (c) If $2^n - 1$ is a prime, then n is a prime number.

7. Let $n = p^k$ where p is a prime and $k > 0$. Compute the sum of all positive divisors of n.

8. Consider the elliptic curve variant of the Diffie-Hellman key exchange protocol. Suppose Alice chooses random secret $n_a = 11$, Bob chooses $n_b = 7$. Public information contains an elliptic curve $E : y^2 = x^3 + 4x + 20 \pmod{29}$ and its point $P = (1, 5)$. Show in detail steps of the protocol.