IV054 Coding, Cryptography and Cryptographic Protocols
2013 - Exercises VIII.

1. (a) Prove that all Carmichael numbers are odd.
   (b) Show that 10585 is a Carmichael number.

2. Consider the elliptic curve $E: y^2 = x^3 + 6x^2 + 14x + 16$ over $\mathbb{Z}_{29}$.
   (a) Verify that the point $P = (8, 3)$ lies on E.
   (b) Using a transformation into the form $y^2 = x^3 + ax + b$ compute the point $2P$.

3. Use the ρ-method with $f(x) = x^2 + 1$ and $x_0 = 5$ to find a factor of $n = 37399$.

4. Decide whether $n^3 + (n + 1)^3 + (n + 2)^3 \equiv 0 \pmod 9$ for any non-negative integer n. Explain your reasoning.

5. Let $n = 561$. Note that $\gcd(2, n) = 1$ and $2^{n-1} \equiv 1 \pmod n$.
   (a) Show that the Rabin-Miller method with $a = 2$ demonstrates that n is composite.
   (b) Show that this witness for the compositeness allows one to factorize n.

6. Prove the following theorem:
   If there exists an integer a such that $a^{n-1} \equiv 1 \pmod n$ and $a^{(n-1)/k} \not\equiv 1 \pmod n$ for all primes $k|(n - 1)$ then n is prime.

7. (a) How many points P such that $2P = \infty$ can be found on non-singular elliptic curves? Does there always exist at least one? Why?
   Consider for both curves over $\mathbb{R}$ and over Z_p, p prime.
   (b) Prove that on a non-singular elliptic curve over $\mathbb{Z}_p$, p prime, for any two different points P_1, P_2 there exists exactly one point P_3 such that $P_1 + P_2 + P_3 = \infty$ (using the addition formulas given at the lecture will not be classified as a proof).
   (c) Prove or disprove that for P_3 as described in (b): $P_1 \neq P_3 \wedge P_2 \neq P_3$.
   (d) Assume you are given $p > 3$ prime and b for the elliptic curve $y^2 = x^3 + ax + b$. How many values of a can be ruled out if you know the curve is non-singular? Discuss possible values for a pair of b, p.
   (e) Suppose you are trying to figure out the order of a subgroup on an elliptic curve over $\mathbb{Z}_{|}$, p prime, generated by a point P. While counting, you find out that kP and $kP + P$ have the same value of x, and this is the first time this has occurred. Can the order of the group be claimed now?
   (f) Find a non-singular elliptic curve over $\mathbb{Z}_{17}$ for which $P = (0, 6)$ is a primitive point (a guess with verification that it is indeed correct is sufficient). Identify all primitive points of the curve you give.