IV054 Coding, Cryptography and Cryptographic Protocols
2017 - Exercises III.

1. Consider the polynomial $g(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$.
   (a) Show that $g(x)$ is the generating polynomial of a binary cyclic code of length 23.
   (b) Find the dimension of the code.
   (c) Find the parity check polynomial.
2. Let C be a binary cyclic code of odd length n. Show that C contains a codeword of odd weight if and only if $\underbrace{11\ldots1}_{n}$ is in C.
3. Consider a binary cyclic code C with a generator polynomial $g(x)$.
   Show that this code is contained in the single-parity-check binary code if and only if $g(1) = 0$.
   Hint: The binary single-parity-check code has the generator polynomial $x + 1$.
4. Consider the polynomial $g(x) = x^2 - 1$ from $F_q[x]$.
   (a) Show that $g(x)$ is the generating polynomial of a q-ary cyclic code of length $5 \cdot 2^n$ for any integer $n \geq 1$ and a prime q.
   (b) Find the dimension of this code.
   (c) Find the parity check polynomial.
5. Prove two following statements:
   (a) For any polynomial $f(x) \in F_q[x]$ the fact that $f(x)$ is irreducible implies that $f(x)$ has no roots in F_q.
   (b) For $f(x) \in F_q[x]$ with $deg(f(x)) \leq 3$ it holds that $f(x)$ has no roots in F_q implies that $f(x)$ is irreducible.
6. For any $m, n, k, d \in \mathbb{N}$, $d > 1$ and q a power of a prime, show that if a cyclic q-ary $[n, k, d]$-code exists then a cyclic q-ary $[mn, mk, d]$-code exists as well.
7. In the lecture we have defined linear codes over all finite fields $GF(q)$. Finite fields with q prime are easy to define – elements of such field $GF(q)$ are $\{0, \ldots, q - 1\}$ and addition and multiplication are defined as addition and multiplication modulo q.

   In fact, however, construction of finite fields $GF(q)$ is known for each $q = p^n$, where p is a prime. After introducing rings of polynomials in this lecture, construction of such fields was introduced on slide 12.

   Given a prime power $q = p^n$ with p prime and $n > 1$, the field $GF(q)$ may be explicitly constructed in the following way. One first chooses an irreducible polynomial $P(x)$ in $F_p[x]$ of degree n (such an irreducible polynomial always exists).

   The elements of $GF(q)$ are the polynomials in $F_p[x]/P(x)$ whose degree is strictly less than n. The addition and the subtraction are those of polynomials over $GF(p)$. The product of two elements is the remainder of the Euclidean division by $P(x)$ of the product in $F_p[x]$.

   (a) How many irreducible polynomials of degree 2 are there in $GF(3)$? List these polynomials.
   (b) Find the multiplication table for $GF(9)$.