Math 406
Assignment 5 (Optional)

Note: Problems marked with an asterisk (*) are only for graduate students.

1. Let $C$ be an $[n, k, d]$ GRS code over a finite field $F$, with $1 < k < n - 1$.
   (a) Show that $C$ is a proper subset (i.e., subcode) of an $[n, k + 1, d - 1]$ GRS code over $F$.
   (b) Given any code $C \subset F^n$ and a $y \in F^n$, define
   \[ d(y, C) = \min \{d(y, c) : c \in C\} \]
   to be the Hamming distance between $y$ and (the closest codeword in) $C$. If $C$ is a GRS code as above, deduce from part (a) that there exists a $y \in F^n$ such that $d(y, C) \geq d - 1$.
   (c) The covering radius of a code $C \subset F^n$ is defined to be the largest distance $d(y, C)$ among all $y \in F^n$. In other words, $\rho(C) := \max \{d(y, C) : y \in F^n\}$. Part (b) shows that the covering radius of a GRS code of type $[n, k, d]$ is at least $d - 1$. Prove that it is, in fact, equal to $d - 1$. [Hint: Show that the covering radius of an MDS code must be strictly less than its minimum distance.]

2. Consider a conventional Reed-Solomon $[n, k, d]$-code $C = C_{\alpha, b, k}$ over $F$, with parity-check matrix defined via an $\alpha \in F$ of order $n$, and an integer $b$. We showed in class that the generator polynomial of $C$ is given by $g_C(X) = \prod_{i=b}^{b+n-k-1}(X - \alpha^i)$. Write $g_C(X)$ as $g_0 + g_1X + \ldots + g_{n-k}X^{n-k}$.
   (a) Show that $g_j \neq 0$ for $0 \leq j \leq n - k$.
   [Hint: Why must $(g_0, g_1, \ldots, g_{n-k}, 0, \ldots, 0) \in F^n$ be a codeword in $C$ of weight equal to $n - k + 1$?]
   (b) Show that the dual code $C^\perp$ of $C$ is a conventional Reed-Solomon code of type $[n, n - k, k + 1]$ over $F$, with generator polynomial $g_{C^\perp}(X) = \prod_{i=1}^{k}(X - \alpha^{i-b})$.

3. (a) Let $C_1, C_2 \subset F^n$ be two linear cyclic $n$-codes with generating polynomials $g_1(X)$ and $g_2(X)$. Show that $C_1 \cap C_2$ and $C_1 + C_2$ are also cyclic, and find their generating polynomials.
   (b) Let $E/F$ be a finite field extension. If $C \subset E^n$ is a cyclic code, show that the subfield sub-code $C \cap F^n$ is a cyclic code.
4. Let \( \alpha \) be a root of \( f(X) = X^6 + X^5 + 1 \) as in Q6 of Assignment 4, and let \( C \) be the binary cyclic code of length 63 with roots \( \alpha \) and \( \alpha^3 \). Thus, \( C \) has (symbolic) parity check matrix
\[
\begin{pmatrix}
1 & \alpha & \alpha^2 & \ldots & \alpha^{62} \\
1 & \alpha^3 & (\alpha^3)^2 & \ldots & (\alpha^3)^{62}
\end{pmatrix}
\]
Find the generating polynomial \( g_C(X) \in \mathbb{F}_2[X] \) of this code, using the fact that \( \Phi_{2^1}(X) = (X^6 + X^5 + X^4 + X^2 + 1)(X^6 + X^4 + X^2 + X + 1) \).

5. Let \( F \) be the splitting field of the polynomial \( X^{13} - 1 \) over the field \( \mathbb{F}_3 \).
   (a) Identify the field.
   (b) Find all the possible values for the dimensions of a cyclic code of length 13 over \( \mathbb{F}_3 \) and the number of such codes for every given dimension.

6*. Let \( \alpha \) be a generator of \( \mathbb{F}_{2^r} \), where \( r \geq 1 \). In the following, the degree of an element in \( \mathbb{F}_{2^r} \) always refers to its degree of its minimal polynomial over \( \mathbb{F}_2 \).
   (a) Show that for \( 0 \leq i \leq 2^r - 1 \), the degree of \( \alpha^i \) is equal to the number of distinct cyclic shifts of the coefficients \( (a_0, \ldots, a_{r-1}) \) of the binary expansion of \( i \). (Thus, \( a_j \in \{0,1\} \) and \( \sum_{j=0}^{r-1} a_j 2^j = i \).
   [Hint: If \( (b_0, b_1, \ldots, b_{r-1}) \) is the binary \( r \)-tuple representation of \( i \), then what is the binary \( r \)-tuple representation of \( 2i \pmod{(2^r - 1)} \)?]
   (b) Deduce from (a) that if \( 1 \leq i \leq 2^{\lfloor r/2 \rfloor} \), then the degree of \( \alpha^i \) is precisely \( r \).
   (c) From (b), we have that for \( r > 2 \), the degree of \( \alpha^3 \) is \( r \). What is the degree of \( \alpha^3 \) when \( r = 2 \)?

7. MAPLE problem (refer to the MAPLE instruction sheet):
   Let \( F = \mathbb{F}_p[x]/(f) \), where \( f \) is an irreducible polynomial of degree \( r \).
   (a) Write a small program \( \text{ord}(a, f, p) \) which computes the order of an element \( a \in F^\times \).
   Test your program for the case \( a = x^2 - x, f = x^3 - x + 1, p = 3 \) and for the case \( a = 2, f = x \) and \( p = 23 \).
   (b) Write a program \( \text{gen}(a, b, k, f, p) \) which computes the generating polynomial \( g_{a,b,k}(X) \) of the conventional Reed-Solomon Code \( C_{a,b,k} \) with \( a \in F^\times \), \( b \in \mathbb{Z} \) and \( k \geq 1 \). (Use your program \( \text{ord} \) from part (a).)
   Test your program for the case \( a = x^2 - x, b = 1, k = 8, f = x^3 - x + 1, \text{ and } p = 3 \) and for the case \( a = 2, b = 3, k = 6, f = x \) and \( p = 23 \).
   (c) Let \( g(X) \in F[X] \) be a generating polynomial of a conventional RS code. Write a program \( \text{encode}(u, g, f, p) \) which implements the encoding procedure (using polynomial multiplication) attached to \( g \). Here \( u \in F^k \) in a source word, and your program should return a code word \( c \in C_g \subset F^n \), where \( C_g \) is the RS-code defined by \( g \).
   Test your program for \( u = [1, 2, 3, 4, 5, 6], g = X^5 + 5X^4 + 14X^3 + 12X^2 + 12X + 15, f = x \) and \( p = 23 \).