Problem 1 (optional Subfield from characteristic) Let $\lambda$ be the characteristic of a Galois field $GF(q)$. Let 1 be the unit element of $GF(q)$. Show that the set

$$S = \left\{ 1, \sum_{i=1}^{2} 1, \sum_{i=1}^{2} \lambda, \ldots, \sum_{i=1}^{\lambda-1} 1, \sum_{i=1}^{\lambda} 1 = 0 \right\}$$

is a subfield of $GF(q)$.

Problem 2 (optional Finding irreducible polynomials) The objective of this problem is to check that you know how to construct a finite field. The procedure can be a little painful by hand, and you are welcome to use Matlab to save time. If you do so, make sure you indicate the principle of your algorithm.

(a) Find all the polynomials of degree 2 and 3 that are irreducible over $GF(2)$ and $GF(3)$. Identify the irreducible polynomials that are primitive.

(b) Construct $GF(9)$ using one of the primitive polynomials identified in part (a).

Problem 3 (Square roots) In a finite field, we say that $y$ in the square root of $x$ if $x^2 = x$. We say that $y$ is the $p$-th root of $x$ if $y^p = x$.

(a) Show that all the elements in $GF(2^m)$ have square roots.

(b) Show that all the elements in $GF(p^m)$ have $p$th roots.

Problem 4 (Solving equations in finite fields) Consider $GF(16)$ with primitive elements $\alpha$ satisfying $\alpha^4 + \alpha + 1 = 0$.

(a) Find all solutions to the simultaneous equations $x + y = \alpha^3$ and $x^2 + y^2 = \alpha^6$.

(b) Find all solutions to the simultaneous equations $x + y = \alpha^3$ and $x^2 + y^2 = \alpha$.

Problem 5 (Subfields in finite fields) Let $\alpha$ be a primitive element of $GF(64)$. It is easy to see $GF(2) = \{0,1\} \subseteq GF(64)$. Find $GF(4)$ and $GF(8)$ in terms of $\alpha$ as subsets of $GF(64)$.

Problem 6 (Reciprocals of polynomials) Let $f(x)$ be a polynomial of degree $n$ over $GF(2)$. The reciprocal of $f(x)$ is defined as

$$f^*(x) = x^{n} f(x^{-1})$$

(a) Prove that $(f^*)^*(x) = f(x)$

(b) Let $f(x)$ be a polynomial with non-zero constant term. Prove that $f(x)$ is irreducible over $GF(2)$ if and only if $f^*(x)$ is irreducible over $GF(2)$

(c) Let $f(x)$ be a polynomial with non-zero constant term. Prove that $f(x)$ is primitive over $GF(2)$ if and only if $f^*(x)$ is primitive.

Problem 7 (optional Minimal polynomials in $GF(32)$) Construct $GF(32)$ and determine the minimal polynomials of all elements.

Problem 8 (optional Binary BCH code of length 31) Determine the dimension and generator polynomial of all the narrow-sense binary BCH codes of length 31.
Problem 9 (Decoding length 31 BCH code) Suppose that the double-error-correcting narrow-sense binary BCH code of length 31 is used over a binary symmetric channel. Decode the received polynomials $x^7 + x^{30}$ and $1 + x^{17} + x^{28}$.

Problem 10 (Optional Decoding length 15 BCH code) The primitive, narrow-sense, triple-error-correcting (15,5) BCH code is being used over a binary symmetric channel. Decode the received vector [00001101000100].

Problem 11 (Exact minimum distance) Let $C$ be the $t$-error correcting narrow-sense binary BCH code of length $n = 2^m - 1$. If $(2t + 1)|n$, show that $x^{n+1}/x^{l+1}$ (with $l = n/(2t + 1)$) is a codeword of $C$. What is the exact minimum distance of $C$?

Problem 12 (BCH code with specific roots) Let $C$ be a length $n$ binary BCH code with the following consecutive zeros ($\alpha$ is primitive $n$-th root of unity)

$$\alpha^{-t} \ldots \alpha^{-1}, \alpha^0, \alpha^1, \ldots, \alpha^t$$

(a) Obtain a lower bound for the minimum distance of $C$ using the BCH bound

(b) if $t$ is odd, show that $\alpha^{-t-1}$ and $\alpha^{t+1}$ are also zeros of $C$

(c) Obtain a better lower bound for the minimum distance when $t$ is odd.

Problem 13 (Nested BCH codes) Show that BCH codes are nested, that is for a fixed $b$ (in the construction), if $C_1$ is a BCH code with design distance $\delta_1$ and $C_2$ is another BCH code with design distance $\delta_2 \geq \delta_1$, then $C_2 \subseteq C_1$. (Hint: you might want to use the result about nested cyclic codes seen in a previous problem set)