Problem 5.1 (Euclidean division algorithm).
(a) For the set \( F[x] \) of polynomials over any field \( F \), show that the distributive law holds:
\[
(f_1(x) + f_2(x))h(x) = f_1(x)h(x) + f_2(x)h(x).
\]
(b) Use the distributive law to show that for any given \( f(x) \) and \( g(x) \) in \( F[x] \), there is a unique \( q(x) \) and \( r(x) \) with \( \deg r(x) < \deg g(x) \) such that \( f(x) = q(x)g(x) + r(x) \).

Problem 5.2 (unique factorization of the integers).
Following the proof of Theorem 7.7, prove unique factorization for the integers \( \mathbb{Z} \).

Problem 5.3 (finding irreducible polynomials).
(a) Find all prime polynomials in \( F_2[x] \) of degrees 4 and 5. [Hint: There are three prime polynomials in \( F_2[x] \) of degree 4 and six of degree 5.]
(b) Show that \( x^{16} + x \) factors into the product of the prime polynomials whose degrees divide 4, and \( x^{32} + x \) factors into the product of the prime polynomials whose degrees divide 5.

Problem 5.4 (The nonzero elements of \( F_{g(x)} \) form an abelian group under multiplication).
Let \( g(x) \) be a prime polynomial of degree \( m \), and \( r(x), s(x), t(x) \) polynomials in \( F_{g(x)} \).
(a) Prove the distributive law, i.e., \( (r(x) + s(x)) \ast t(x) = r(x) \ast t(x) + s(x) \ast t(x) \). [Hint: Express each product as a remainder using the Euclidean division algorithm.]
(b) For \( r(x) \neq 0 \), show that \( r(x) \ast s(x) \neq r(x) \ast t(x) \) if \( s(x) \neq t(x) \).
(c) For \( r(x) \neq 0 \), show that as \( s(x) \) runs through all nonzero polynomials in \( F_{g(x)} \), the product \( r(x) \ast s(x) \) also runs through all nonzero polynomials in \( F_{g(x)} \).
(d) Show from this that \( r(x) \neq 0 \) has a mod-\( g(x) \) multiplicative inverse in \( F_{g(x)} \); i.e., that \( r(x) \ast s(x) = 1 \) for some \( s(x) \in F_{g(x)} \).

Problem 5.5 (Construction of \( F_{32} \)).
(a) Using an irreducible polynomial of degree 5 (see Problem 5.3), construct a finite field \( F_{32} \) with 32 elements.
(b) Show that addition in \( F_{32} \) can be performed by vector addition of 5-tuples over \( F_2 \).
(c) Find a primitive element \( \alpha \in F_{32} \). Express every nonzero element of \( F_{32} \) as a distinct power of \( \alpha \). Show how to perform multiplication and division of nonzero elements in \( F_{32} \) using this “log table.”
(d) Discuss the rules for multiplication and division in $F_{32}$ when one of the field elements involved is the zero element, $0 \in F_{32}$.

**Problem 5.6 (Second nonzero weight of an MDS code)**

Show that the number of codewords of weight $d + 1$ in an $(n, k, d)$ linear MDS code over $F_q$ is

$$N_{d+1} = \binom{n}{d+1} \left( q^2 - 1 \right) - \binom{d+1}{d} (q - 1),$$

where the first term in parentheses represents the number of codewords with weight $\geq d$ in any subset of $d + 1$ coordinates, and the second term represents the number of codewords with weight equal to $d$.

**Problem 5.7 ($N_d$ and $N_{d+1}$ for certain MDS codes)**

(a) Compute the number of codewords of weights 2 and 3 in an $(n, n - 1, 2)$ SPC code over $F_2$.

(b) Compute the number of codewords of weights 2 and 3 in an $(n, n - 1, 2)$ linear code over $F_3$.

(c) Compute the number of codewords of weights 3 and 4 in a $(4, 2, 3)$ linear code over $F_3$.

**Problem 5.8 (“Doubly” extended RS codes)**

(a) Consider the following mapping from $(F_q)^k$ to $(F_q)^{q+1}$. Let $(f_0, f_1, \ldots, f_{k-1})$ be any $k$-tuple over $F_q$, and define the polynomial $f(z) = f_0 + f_1 z + \cdots + f_{k-1} z^{k-1}$ of degree less than $k$. Map $(f_0, f_1, \ldots, f_{k-1})$ to the $(q + 1)$-tuple $(\{f(\beta_j), \beta_j \in F_q\}, f_{k-1})$—i.e., to the RS codeword corresponding to $f(z)$, plus an additional component equal to $f_{k-1}$.

Show that the $q^k (q + 1)$-tuples generated by this mapping as the polynomial $f(z)$ ranges over all $q^k$ polynomials over $F_q$ of degree less than $k$ form a linear $(n = q + 1, k, d = n - k + 1)$ MDS code over $F_q$. [Hint: $f(z)$ has degree less than $k - 1$ if and only if $f_{k-1} = 0$.]

(b) Construct a $(4, 2, 3)$ linear code over $F_3$. Verify that all nonzero words have weight 3.