31 (First order Reed–Muller codes). Let $L_m$ be the vector space of polynomials of degree $\leq 1$ in $m$ indeterminates and with coefficients in $F$. Thus the elements of $L_m$ are expressions $a_0 + a_1X_1 + \cdots + a_mX_m$, where $X_1, \ldots, X_m$ are indeterminates and $a_0, a_1, \ldots, a_m$ are arbitrary elements of $F$. So $1, X_1, \ldots, X_m$ is a basis of $L_m$ over $F$ and, in particular, the dimension of $L_m$ is $m + 1$.

Let $n$ be an integer such that $q^{m-1} < n \leq q^m$ and pick distinct vectors

$$\mathbf{x} = \mathbf{x}^1, \ldots, \mathbf{x}^n \in F^m.$$ 

Show that:

1) The linear map

$$\varepsilon: L_m \rightarrow F^n, \quad \varepsilon(f) = (f(\mathbf{x}^1), \ldots, f(\mathbf{x}^n))$$

is injective.

2) The image of $\varepsilon$ is a linear code of type $[n, m + 1, n - q^{m-1}]$. 
Such codes are called \textit{(first order) Reed–Muller codes} and will be denoted \(RM_1^X(m)\). In the case \(n = q^m\), instead of \(RM_1^X(m)\) we will simply write \(RM_1(m)\) and we will say that this is a \textit{full Reed–Muller code}. Thus \(M_1(m) \sim [q^m, m + 1, q^{m-1}(q - 1)]\).

\textbf{32.} Let \(C\) be the binary code generated by the matrix

\[
G = \begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1
\end{pmatrix}.
\]

Construct a table of syndrome-leaders and use it to decode \(110101101101110111000\).
33. Let $C$ be the binary code generated by the matrix

$$G = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}.$$  

Prove that for any $y \in B^{10}$ there is a unique vector $x \in C$ such that $hd(y, x)$ is minimum.

34. Show that for binary linear codes of length $n$, and a binary symmetric channel with a probability $p$ of a bit error,

a) the probability of a correct decoding with the syndrome-leader decoder is

$$P_c = \sum_{j=0}^{t} \binom{n}{j} p^j(1 - p)^{n-j} + \sum_{j=t+1}^{n} \alpha_j p^j(1 - p)^{n-j},$$
where $\alpha_j$ is the number of leaders of weight $j$. Deduce that the dominant term (assuming $p$ small) of the probability of a decoding error is

$$\left(\binom{n}{j} - \alpha_{t+1}\right) p^{t+1}.$$

b) Prove that the probability of an idetectable error is

$$\sum_{j=d}^{n} A_j p^j (1 - p)^{n-j},$$

where $A_j$ is the number of code vectors of weight $j$. 
Let $H$ be the control matrix of a binary linear code and $E$ a leader’s table.

**a)** Consider the following *incremental decoding* algorithm:

1. Set $j = 1$.
2. Let $w = |E(yH^T)|$, the weight of the leader class of the syndrome $yH^T$.
3. If $w = 0$, return $y$.
4. Otherwise, if the weight of the class leader of the syndrome $(y + \varepsilon_j)H^T$ is $< w$, set $y = y + \varepsilon_j$, $j = j + 1$.
5. If $j = n$, stop, else, go to 2.

Show that this decoder coincides with the syndrome-leader decoder corresponding to the table $E$.

**b)** Generalize the incremental decoding algorithm for linear codes over any finite field.
36. Let $a = \sum_{j=0}^{23} a_j t^j$ and $\bar{a} = \sum_{j=0}^{24} \bar{a}_j t^j$ be the weight enumerators of the binary Golay code $C$ and of its parity completion $\bar{C}$.

1. Prove that $a_j = a_{23-j}$, $j = 0, \ldots, 23$, and that $\bar{a}_j = \bar{a}_{24-j}$, $j = 0, \ldots, 24$.

2. Using 1, show that the minimum distance of $\bar{C}$ is 8, and using that $\bar{C}$ has only even-weight vectors, obtain that $\bar{a}$ has the form
   
   $$\bar{a} = 1 + \bar{a}_8 t^8 + \bar{a}_{10} t^{10} + \bar{a}_{12} t^{12} + \bar{a}_{10} t^{14} + \bar{a}_8 t^{16} + t^{24}.$$

3. Use now the MacWilliams identities to show that
   
   $$\bar{a}_8 = 759, \bar{a}_{10} = 0, \bar{a}_{12} = 2576.$$

4. Establish that
   
   $$a_7 + a_8 = \bar{a}_8, \ a_9 = a_{10} = 0 \ i \ a_{11} = a_{12} = \bar{a}_{12}/2.$$

5. Prove that
   
   $$a_7 = 253 \ and \ a_8 = 506,$$
so that
\[ a = 1 + 253t^7 + 506t^8 + 1228t^{11} + 1288t^{12} + 506t^{15} + 253t^{16} + t^{23} \]

[Calculate \( a_7 \) directly, observing that for each word of weight 4 there is exactly a code word of weight 7 containing it]

37. A \( q \)-ary erasure channel is a \( q \)-ary channel for which some of the received vector components can be the symbol \(?\), in which case we say that we have an erasure in the corresponding position. If we use, with this channel, a linear code \( C \sim [n, k, d]_q \), prove that it is possible to correct \( e \) errors and \( f \) erasures if and only if \( 2e + f \leq d - 1 \).

38. Prove that \( \varphi(n) \) is even for all \( n > 2 \) and find the sets \( \{n \in \mathbb{Z}^+ | \varphi(n) = m\} \) for \( m = 1, 2, 4 \).
39. The four groups $\mathbb{Z}_5^*$, $\mathbb{Z}_8^*$, $\mathbb{Z}_{10}^*$ and $\mathbb{Z}_{12}^*$ have order 4. Determine which are cyclic and which are isomorphic to the Klein group (the only two possibilities for groups of order 4).

40. Prove that the values of $n$ for which $|\mathbb{Z}_n^*| = 6$ are 7, 9, 14 and 18. As any group of order 6 is cyclic, the groups $\mathbb{Z}_7^*$, $\mathbb{Z}_9^*$, $\mathbb{Z}_{14}^*$ and $\mathbb{Z}_{18}^*$ are isomorphic. Find an isomorphism between $\mathbb{Z}_7^*$ and each of the other three groups.

41. Prove that the values of $n$ for which $|\mathbb{Z}_n^*| = 8$ are 15, 16, 20, 24 and 30. Prove that $\mathbb{Z}_{24}^*$ is isomorphic to $\mathbb{Z}_3^2$ and that the other four groups are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$. Find and isomorphism between $\mathbb{Z}_{15}^*$ and $\mathbb{Z}_{16}^*$. 
42. For each \( k = 1, 2, 3, \ldots \) let \( p_k \) be the \( k \)-th prime number and set

\[
N_k = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1) \quad \text{and} \quad P_k = p_1 p_2 \cdots p_k.
\]

Prove that the minimum of \( \varphi(n)/n \) on the interval \( (P_k) \ldots (P_{k+1} - 1) \) is \( N_k/P_k \). Deduce from this that in the interval \( 2 \ldots (2 \times 10^{11}) \) we have \( \varphi(n)/n > 0.1579 \). On the other hand, prove that \( \lim \inf_{n \to \infty} \frac{\varphi(n)}{n} = 0 \).

43. a) Let \( F \) be a finite field and \( K \) a subfield. Set \( q = |K| \) and let \( r \) be the positive integer such that \( |F| = q^r \). Let \( f \in K[X] \) be a monic irreducible polynomial of degree \( r \) and \( \beta \in F \) such that \( f(\beta) = 0 \). Prove that there exists a unique \( K \)-isomorphism \( K[X]/(f) \cong F \) such that \( x \mapsto \beta \), where \( x \) is the class of \( X \mod f \).

b) The polynomials \( f = X^3 + X + 1 \) and \( g = X^3 + X^2 + 1 \) are irreducible over \( \mathbb{Z}_2 \). Find all isomorphisms between \( \mathbb{Z}_2[X]/(f) \) and \( \mathbb{Z}_2[X]/(g) \).
44. Let $K$ be a finite field, $\alpha, \beta \in K^r$, $r = \text{ord}(\alpha)$, $s = \text{ord}(\beta)$. Let
\[ t = \text{ord}(\alpha \beta), \quad d = \text{mcd}(r, s), \quad m = \text{mcm}(r, s), \quad m' = m/d. \]
Prove that $m'|t$ and $t|m$. Thus $\text{ord}(\alpha \beta) = rs$ if $d = 1$. Find examples for which $d > 1$ and $t = m'$ (respectively $t = m$).

45. Gauss algorithm to find a primitive element $\alpha$ of a field $K$ of $q$ elements:

1. Let $a$ be a non-zero element of $K$ and $r = \text{ord}(a)$. If $r = q - 1$, it is enough to put $\alpha = a$. Thus we may assume that $r < q - 1$.

2. Let $b$ be an element such that $b \not\in \{1, a, \ldots, a^{r-1}\}$ (this can be achieved by selecting an element $x$ of $K$ at random and finding $x^r$; if $x^r \neq 1$, then $x \not\in \{1, a, \ldots, a^{r-1}\}$, and we can take $b = x$; otherwise we try with another $x$).
3. Let \( s \) be the order of \( b \). If \( m = q - 1 \), we can set \( \alpha = b \). Otherwise we have \( s < q - 1 \). In this case, calculate positive integers \( d \) and \( e \), starting with \( d = e = 1 \), in the following way: examine successively the prime divisors \( p \) of \( r \) and \( s \) and set, if \( m \) is the minimum of the exponents of \( p \) in \( r \) and \( s \), \( d := dp^m \) if \( m \) is reached for \( r \) (in this case \( p \) appears in \( s \) with exponent at least \( m \)) and \( e := ep^m \) if \( m \) is reached for \( s \) (in this case \( p \) appears in \( r \) with exponent higher than \( m \)).

4. Substitute \( a \) by \( a^d b^s \) and reset \( r = \text{ord}(a) \). If \( r = q - 1 \), we can take \( \alpha = a \). Otherwise we go back to step 2.

Prove that this algorithm ends in a finite number of steps (show that the ordre of \( a^d b^s \) in step 4 is \( \text{mcm}(r, s) \) and that \( \text{mcm}(r, s) > \max(r, s) \)).