B7.

[20 marks]

1. Let C be a cyclic code and consider it as an ideal in $R_n = \mathbb{F}_p[x]/(x^n - 1)$ in the usual way. Prove that there is a unique monic polynomial $g \in \mathbb{F}_p[x]$ of minimum degree such that $C = \bar{g}R_n$.
2. Prove that g divides $x^n - 1$.
3. Write down an expression for the dimension of C in terms of g and n.

   Given that, over $\mathbb{F}_3$,

   $$x^8 - 1 = (x^5 + x^4 + x^3 - x^2 + 1)(x^3 - x^2 - 1) :$$

4. Write down a generator polynomial and a check polynomial for a ternary cyclic code of length 8 and dimension 5.
5. Write down a generator matrix and a parity check matrix for this code.
6. Find the minimum distance of this code.
7. Are either of the vectors 11000000 or 11102000 in this code?
8. The repetition code in $\mathbb{F}_p^{(n)}$ is always a cyclic code. Write down a generator matrix and a check polynomial for the repetition code.

B8.

[20 marks]

1. Given two codes C_1 and C_2 in $F^{(n)}$, define the code $|C_1|C_2|$.
2. Prove that $d(|C_1|C_2|) = \min\{2d(C_1), d(C_2)\}$.
3. Define the rth order binary Reed-Muller code $R(r, m)$ in terms of Boolean functions.
4. Show that $R(r + 1, m + 1) = |R(r + 1, m)|R(r, m)|$.
5. Find a generator matrix and a parity check matrix and the distance for the code $R(2, 3)$ (you may quote any result from the course without proof).
6. Both $R(0, m)$ and $R(m - 1, m)$ are well-known codes with their own names. What are these names (or give a simple description of these codes)?

END OF EXAMINATION PAPER