# Exercices du cours de Théorie de l'Information et Codage

cours 11 du 11 mai 2010.

1. Pour $p = 2$ et $n = 2^m - 1$ (avec $m \geq 3$), montrer que les classes cyclotomiques modulo $n$, $C_1$ et $C_3$ sont distinctes et $|C_1| = |C_3| = m$. Donc les polynômes $M^{(1)}$ et $M^{(3)}$ sont premiers entre eux de degrés $m$.

2. Soit $\mathcal{C}$ un code cyclique de polynôme générateur $g(x)$ et de polynôme vérificateur $h(x) = (x^n - 1)/g(x)$. Montrer que le code dual de $\mathcal{C}$ est cyclique et a pour polynôme générateur $g^{\perp}(x) = x^{deg(h(x))}h(x^{-1})$.

3. Montrer que les zéros de $x^n - 1$ forment un sous-groupe cyclique de $GF(q^m)^*$.

4. Montrer qu'un code cyclique de longueur $n$ avec comme zéros $\alpha^b, \alpha^{b+r}, \alpha^{b+2r}, \ldots, \alpha^{b+(\delta-2)r}$ où $r \wedge n = 1$ a pour distance miniale $d \geq \delta$.