CONTRÔLE CONTINU N° 1

NOM Prénom : ....

Numéro d'étudiant : ....

Soient q une puissance d'un nombre premier, n un nombre **premier** tel que $(n, q) = 1$ et soit m l'ordre de q modulo n.

a) Montrer que pour tout $s \neq 0 \bmod n$ et pour tout entier i,
$$sq^i = s \bmod n \Leftrightarrow q^i = 1 \bmod n.$$

b) En déduire que pour tout $s \neq 0 \bmod n$ les classes cyclotomiques C_1 et C_s ont la même cardinalité.

c) En déduire qu'il existe un entier t tel que $n - 1 = mt$ et que le nombre des codes cycliques de longueur n sur $\mathbb{F}_q$ est égale à 2^{t+1}.

Considérons maintenant $q = 2$ et $n = 31$.

d) Montrer que les dimensions possibles des codes cycliques de longueur 31 sur $\mathbb{F}_2$ sont $0, 1, 5, 6, 10, 11, 15, 16, 20, 21, 25, 26, 30, 31,$ c'est-à-dire tout entier dans $\{0, \ldots, 31\}$ qui sont égaux à 0 ou 1 modulo 5.

e) Soit $\mathcal{C} := \langle x + 1\rangle$. Montrer que $\mathcal{C}$ est le code de parité de longueur 31. Quels sont ses paramètres ?

f) Soit $g(x) := x^5 + x^2 + 1$ un facteur irréductible de $x^{31} + 1$. Écrire le polynôme de contrôle de $\mathcal{C} := \langle g(x)\rangle$. En déduire que $\mathcal{C}$ est le code de Hamming $\mathcal{H}_5$.

NOM Prénom : ....

Numéro d'étudiant : ....

NOM Prénom : ....

Numéro d'étudiant : ....