

d'ordre d_1 .

b) Montrer que le nombre de générateurs de G_d est $\varphi(d_1)$.
Soit N_d le nombre de générateurs de G_d . Montrer que $\{N_d, d|n\}$ réalise une partition de $\mathbb{Z}/n\mathbb{Z}$. En déduire la relation :

$$n = \sum_{d|n} \varphi(d).$$

3°. a) Montrer que si A est un anneau alors $(U(A), \cdot)$ est un groupe. En déduire que, si x est inversible dans $\mathbb{Z}/n\mathbb{Z}$, alors $x^{\varphi(n)} = 1$. Montrer aussi que, si $p \equiv 1 [\varphi(n)]$ alors $x^p = x$.

b) On rappelle le théorème de Fermat : si x n'est pas divisible par p nombre premier, alors $p \mid x^{p-1} - 1$. Montrer alors que si $n \equiv 1 [p-1]$: $p \mid x^n - x$.

c) Si K est un entier sans facteur carré (i.e. $K = p_1 p_2 \dots p_r$ où les p_i sont des nombres premiers distincts) et si $n \equiv 1 [\varphi(K)]$, montrer que $x^n \equiv x [K]$.

d) Soit $\gamma \in \mathbb{N}^*$ tel que $\gamma \wedge \varphi(K) = 1$; on considère la fonction codage qui à $T \in [0, K-1]$ fait correspondre l'unique entier $\mathcal{C}(T) \in [0, K-1]$ tel que $\mathcal{C}(T) \equiv T^\gamma [K]$. Soit aussi $\delta \in \mathbb{N}^*$ tel que $\gamma\delta \equiv 1 [\varphi(K)]$. Montrer alors que la fonction $\mathcal{C}$ admet une fonction réciproque $\mathcal{D}$ ($\mathcal{D}$ pour décodage) définie par : $\mathcal{D}: M \in [0, K-1] \mapsto \mathcal{D}(M) \in [0, K-1] : \mathcal{D}(M) \equiv M^\delta [K]$.

e) Application: $K = 97343$, $\gamma = 7$. Avec l'algorithme d'Euclide, trouver $\delta \in [1, 96719]$ tel que $\gamma\delta \equiv 1 [\varphi(K)]$. Calculer $\mathcal{C}(T)$ pour $T = 183$. Calculer $\mathcal{D}(M)$ pour $M = 1970$.