Exercice - M0218

Soit φ la fonction qui à tout entier naturel non nul n associe le nombre $\varphi(n)$ d'entiers naturels inférieurs à n et premiers avec n. φ est appelée fonction indicatrice d'Euler.

1. a) Calculer $\varphi(1), \varphi(2), \varphi(3), \varphi(4), \varphi(5)$ et $\varphi(6)$
   b) Soit p un nombre premier. Calculer $\varphi(p)$
   c) Soit p un nombre premier et α un entier naturel non nul. Soit q un entier tel que $1 \leq q \leq p^\alpha$. Démontrer que :
   $$\text{PGCD}(q; p^\alpha) \neq 1 \iff p \text{ divise } q$$
   En déduire que :
   $$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$$
2. Pour tout entier non nul n, on note E_n l'ensemble des entiers x premiers avec n tels que $0 \leq x \leq n-1$. $\varphi(n)$ est donc le nombre d'éléments de $E - n$.
   a) Soient $r \in E_n$ et $s \in E_m$. Montrer que le système de congruence (S)
   $$(S) : \begin{cases} x \equiv r \pmod{m} \\ x \equiv s \pmod{n} \end{cases}$$
   admet une infinité de solutions de la forme $x = x_0 + knm$, où x_0 est une solution particulière de (S) et où k est un entier.
   b) Démontrer qu'il existe un unique $\rho \in E_{nm}$ tel que pour tout solution x de (S),
   $$x \equiv \rho \pmod{nm}$$
   A tout couple (r, s) de $E_m \times E_n$, on peut donc associer un unique $\rho \in E_{nm}$
   c) Réciproquement, soit $\rho \in E_{nm}$. Il existe un entier x tel que $x \equiv \rho \pmod{nm}$. Justifier que :
   $$x \equiv \rho \pmod{m} \quad \text{et} \quad x \equiv \rho \pmod{n}$$
   On note r et s les restes respectifs des divisions euclidiennes de ρ par m et par n. Démontrer que :
   $$x \equiv r \pmod{m} \qquad x \equiv s \pmod{n} \qquad r \in E_m \quad s \in E_n$$
   A tout $\rho de E_{nm}$ on peut donc associer un unique couple (r, s) tel que $r \in E_m$ et $s \in E_n$ par la méthode précédement décrite.
   d) Combien y a-t-il de couples (r, s) tels que $r \in E_m$ et $s \in E_n$? Déduire de b) et c) que :
   $$\varphi(nm) = \varphi(n)\varphi(m)$$
   e) Démontrer, en utilisant 1c) et 2d) que, si un entier naturel non nul n admet pour décomposition primaire $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ alors :
   $$\varphi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$
   f) Calculer $\varphi(229320)$
3. Soit n un entier naturel non nul. Un entier a est dit inversible modulo n s'il existe un entier a' tel que $aa' \equiv 1 \pmod{n}$.
   a) Démonter que : a est inversible modulo $n \iff PGCD(a; n) = 1$
   b) En déduire que les éléments inversibles modulo n inférieurs à n sont les éléments de E_n et qu'il y en a exactement $\varphi(n)$.
   c) Déterminer les éléments inversibles moldulo 3, puis ceux inversible modulo 6.
4. Soient n un entier naturel non nul et a un entier premier avec n.
   a) Soit $y \in E_n$. Montrer qu'il existe un unique $x \in E_n$ tel que : $ax \equiv y \pmod{n}$.

b) Démontrer que x est inversible modulo n si et seulement si ax est inversible modulo n.

c) Soit $I = \{x_1, x_2, \cdots, x_m\}$ l'ensemble des éléments de E_n. Démontrer que :

$$x_1 x_2 \cdots x_m \equiv (ax_1)(ax_2)\cdots(ax_m) \pmod{n}$$

d) En déduire le théorème d'Euler : $PGCD(a; n) = 1 \implies a^{\varphi(n)} \equiv 1 \pmod{n}$.

e) Quel cas particulier retrouve-t-on si n est premier ?