MATH

Devoir à la Maison n°7

MPSI 31/01/2025

Préambule

Vous apporterez le plus grand soin à la rigueur et à la rédaction de vos réponses.
Vous êtes invités à **encadrer** ou **souligner** vos réponses.

EXERCICE

L'objectif de cet exercice est de démontrer un théorème d'Euler généralisant le petit théorème de Fermat.
On note $\mathbb{P}$ l'ensemble des nombres premiers et, pour tout $n \in \mathbb{N}^*$, $\mathbb{P}_n$ l'ensemble des nombres entiers de $[\![1, n]\!]$ premiers avec n. On définit ensuite l'*indicatrice d'Euler* en posant, pour tout $n \in \mathbb{N}^*$:

$$\varphi(n) = |\mathbb{P}_n|.$$

Pour tout $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, on note $r(a, b)$ le reste dans la division euclidienne de a par b.

1. Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}$ tel que $n \geqslant 2$. Montrer que a et n sont premiers entre eux si, et seulement si, $r(a, n) \in \mathbb{P}_n$.
2. Montrer que $\forall n \in \mathbb{N}^*$, $\varphi(n) \geqslant 1$ et étudier le cas d'égalité.
3. Calculer $\varphi(p)$ lorsque $p \in \mathbb{P}$.
4. Établir que $\varphi(p^n) = p^{n-1}(p-1)$ pour tout $p \in \mathbb{P}$ et tout $n \in \mathbb{N}^*$.
5. Soient m, n deux entiers supérieurs ou égaux à 2. Pour tout $a \in \mathbb{N}^*$, on pose $f(a) = (r(a, m), r(a, n))$.
   (a) Montrer que l'on définit ainsi une fonction $f : \mathbb{P}_{mn} \to \mathbb{P}_m \times \mathbb{P}_n$.
   (b) On suppose maintenant que m et n sont premiers entre eux.
      i. Montrer que f est injective.
      ii. Soit $(r_m, r_n) \in \mathbb{P}_m \times \mathbb{P}_n$. Justifier l'existence de deux entiers u et v tels :
      $$(r_n - r_m)mu + r_n = (r_m - r_n)nv + r_m.$$
      iii. En déduire que f est surjective.
      iv. En déduire que $\varphi(mn) = \varphi(m)\varphi(n)$.
6. Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. Pour tous $a, k \in \mathbb{P}_n$, on pose $g_a(k) = r(ak, n)$.
   (a) Montrer que, pour tout $a \in \mathbb{P}_n$, $g_a : \mathbb{P}_n \to \mathbb{P}_n$ est bijective.
   (b) Justifier que, si $a \in \mathbb{P}_n$:
   $$\prod_{k \in \mathbb{P}_n} (ak) \equiv \prod_{k \in \mathbb{P}_n} k \quad [n]$$
   et en déduire que $a^{\varphi(n)} \equiv 1\ [n]$.
   (c) En déduire le théorème d'Euler : pour tout $a \in \mathbb{N}$ premier avec n, $a^{\varphi(n)} \equiv 1\ [n]$.
   (d) Justifier l'appelation « généralisation du petit théorème de Fermat » du début du problème.