

EXAMEN - session 1
ARITHMÉTIQUE

*Les calculatrices et les documents sont interdits.
La rédaction sera prise en compte dans la notation.*

Cours. (4,5 points=1+1+1,5+1)

- 1) Donner la définition du ppcm de n entiers relatifs, a_1, \dots, a_n , tous non nuls.
- 2) Énoncer le théorème de Fermat.
- 3) Rappeler la définition de la fonction φ d'Euler puis en donner la valeur de $\varphi(n)$ en fonction de la décomposition en nombres premiers de n .
- 4) Quel est le nombre dont la décomposition en fraction continue est $[2, 2, 2, \dots] = [\bar{2}]$?

Exercice 1 : (3 points)

Résoudre le système suivant :
$$\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv 8 \pmod{28} \end{cases}$$

Exercice 2 : (4,5 points=1+(1+1,5)+1)

Soit $n \geq 1$ un entier naturel.

- 1) Compléter cet énoncé (théorème de Wilson): n est premier si et seulement si n divise \dots

On souhaite prouver ce théorème.

- 2) On suppose que n est premier. On notera \bar{a} la classe dans $\mathbb{Z}/n\mathbb{Z}$ d'un entier a .
 - (i) Résoudre l'équation $x^2 = \bar{1}$ dans $\mathbb{Z}/n\mathbb{Z}$.
 - (ii) Que vaut $\overline{(n-1)!}$? Puis conclure.
- 3) Prouver la réciproque.

Exercice 3 : (4 points=0,5+1+2,5)

On se propose de montrer qu'il existe une infinité de nombres premiers congrus à 5 modulo 6. Par l'absurde on suppose qu'il y en a un nombre fini et on pose $A = \{p \text{ premier} \mid p \equiv 5 \pmod{6}\}$.

- 1) Montrer que A est non vide.

On note donc $A = \{p_1, \dots, p_r\}$ avec $r \geq 1$. Posons $N = (6p_1 \dots p_r) - 1$.

- 2) Soit q un diviseur de N . Justifier que q et 6 sont premiers entre eux.
- 3) Montrer qu'il existe q un nombre premier, diviseur de N tel que $q \equiv 5 \pmod{6}$. Conclure.

Exercice 4 : (4,5 points=0,5+1+1+0,5+1,5)

Soit $n \in \mathbb{N}$ avec $n \geq 1$. On note σ_n l'ensemble des bijections de $\{1, \dots, n\}$ sur lui-même. On dit que $\sigma \in \sigma_n$ est un dérangement si pour tout $i \in \{1, \dots, n\}$, on a $\sigma(i) \neq i$. On note D_n l'ensemble des dérangements. On cherche à déterminer le cardinal de D_n . Pour $i \in \{1, \dots, n\}$, on note $A_i = \{\sigma \in \sigma_n \mid \sigma(i) = i\}$.

- 1) Que vaut le cardinal de σ_n ?
- 2) Que vaut le cardinal de A_i ?
- 3) Pour tout k -uplet d'indices $1 \leq i_1 < \dots < i_k \leq n$, déterminer le cardinal de $A_{i_1} \cap \dots \cap A_{i_k}$?
- 4) Comparer D_n et $\bigcup_{1 \leq i \leq n} A_i$.

5) En déduire que $\text{card}(D_n) = n! - \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} [(n-k)!]$.