

Examen - session 2

ARITHMÉTIQUE

Les calculatrices et les documents sont interdits.

La rédaction sera prise en compte dans la notation.

Cours. (4 points=1+1+2) *Chaque réponse devra être justifiée !*

On rappelle que, pour tout entier $n \geq 1$, la fonction caractéristique d'Euler $\varphi(n)$ est le cardinal de l'ensemble:

$$\{k \in \{1, \dots, n\} \mid \text{pgcd}(k, n) = 1\}.$$

1) Soit p un nombre premier. Que vaut $\varphi(p)$?

2) Soient p un nombre premier et $\alpha \geq 1$ un entier. Que vaut $\varphi(p^\alpha)$?

On rappelle que si n et m sont premiers entre eux, on a $\varphi(nm) = \varphi(n) \cdot \varphi(m)$.

3) Donner une expression de $\varphi(n)$ en fonction de sa décomposition en nombres premiers.

Exercice 1. (5 points=(0,5+1)+3+0,5)

Une comète A , qui peut être observée de la terre tous les 107 ans, était visible en 1996. Une autre comète B , qui est observable de la terre tous les 17 ans, était visible en 2000. On cherche toutes les années $N \geq 2008$ telles que ces deux comètes soient visibles de la terre (toutes les deux la même année!).

1)a) Montrer qu'il s'agit de résoudre le problème (d'inconnue N):

$$N \equiv \alpha [a] \text{ et } N \equiv \beta [b] \text{ et } N \geq 2008$$

où on précisera les valeurs de α , a , β et b .

b) Montrer que c'est équivalent à trouver tous les couples $(n, m) \in \mathbb{Z}^2$ tels que :

$$\beta - \alpha = na - mb \quad \text{avec} \quad m \geq 1.$$

2) Trouver tous les couples $(n, m) \in \mathbb{Z}^2$ tels que $\beta - \alpha = na - mb$.

3) Résoudre le problème de départ.

Exercice 2. (2 points)

Soient n, p des entiers avec $n \geq p$. Montrer que

$$C_p^p + C_{p+1}^p + \cdots + C_n^p = C_{n+1}^{p+1}.$$

Notation: $C_n^k = \binom{n}{k}$.

Exercice 3. (9 points=1,5+(2,5+1)+(1+1)+2)

1) On fixe un entier $n \geq 2$. Soient a, b et $c \in \mathbb{N}$, non nuls, avec $a^b \equiv 1 [n]$ et $a^c \equiv 1 [n]$. Enfin, on désigne par d le pgcd de b et c .

Montrer que $a^d \equiv 1 [n]$.

Soit p un nombre premier tel que $p \equiv 3 [4]$.

2) Supposons qu'il existe un entier a tel que $a^2 \equiv -1 [p]$.

a) En justifiant que l'on peut appliquer le 1. avec $b = 4$ et $c = p - 1$, montrer que $a^2 \equiv 1 [p]$.

b) Quel est l'ensemble des solutions de $a^2 \equiv -1 [p]$?

3) Soient x et y des entiers tels que p divise $x^2 + y^2$.

a) On suppose que p ne divise pas x . Justifier qu'il existe $z \in \mathbb{N}$ tel que $\bar{x}.\bar{z} = \bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. En déduire qu'alors $y^2.z^2 \equiv -1 [p]$.

b) Montrer que p divise x et y .

4) En déduire que si un entier N est somme de deux carrés d'entiers alors les nombres premiers congrus à 3 modulo 4 intervenant dans la décomposition N apparaissent avec un exposant pair.