

Examen du 16 janvier 2018

Durée 2h

**Les documents, calculatrices et téléphones portables sont interdits.**

**Toutes les réponses devront être soigneusement justifiées.**

Les deux exercices sont indépendants.

**Exercice 1**

Les cinq questions sont indépendantes.

- 1) Quel est le plus petit nombre premier plus grand que 50 ?
- 2) Soit  $\varphi$  la fonction indicatrice d'Euler.
  - 2.1) Calculer  $\varphi(100)$ .
  - 2.2) En déduire les deux derniers chiffres intervenant dans l'écriture décimale de  $3^{200}$ .
- 3) Soit  $n \geq 1$  un entier. Étant donné un entier  $a \in \mathbb{Z}$ , quel est l'ordre de la classe de  $a$  dans le groupe additif  $(\mathbb{Z}/n\mathbb{Z}, +)$  ?
- 4) Dans l'anneau  $\mathbb{Z}/175\mathbb{Z}$ , montrer que la classe de 89 est inversible et déterminer son inverse.
- 5) Soient  $K$  un corps fini de cardinal  $q$  et  $\ell$  un nombre premier. Notons  $I_\ell(q)$  le nombre de polynômes irréductibles unitaires de degré  $\ell$  à coefficients dans  $K$ . Que vaut  $I_\ell(q)$  ?

**Exercice 2**

Considérons dans l'anneau  $\mathbb{F}_2[X]$  le polynôme

$$f = X^5 + X^2 + 1.$$

- 1) Déterminer le reste de la division euclidienne de  $f$  par  $X^2 + X + 1$ .
- 2) Expliciter les polynômes irréductibles de degré 1 et de degré 2 dans  $\mathbb{F}_2[X]$ .
- 3) En déduire que  $f$  est irréductible dans  $\mathbb{F}_2[X]$ .

Posons

$$K = \mathbb{F}_2[X]/(f).$$

- 4) Justifier pourquoi  $K$  est un corps.
- 5) Quelle est sa caractéristique ? Quel est son cardinal ?
- 6) Quel est l'ordre de tout élément de  $K^*$  distinct de 1 ?

Soit  $\alpha$  la classe de  $X$  modulo l'idéal  $(f)$ . On rappelle que  $\mathcal{B} = (1, \alpha, \alpha^2, \alpha^3, \alpha^4)$  est une base du  $\mathbb{F}_2$ -espace vectoriel  $K$ .

- 7) Quelles sont les coordonnées de  $\alpha^8$  dans la base  $\mathcal{B}$  ?
- 8) Quel est le plus petit entier naturel  $n$  tel que  $\alpha^n = \alpha^4 + 1$  ?
- 9) En déduire les coordonnées de l'inverse de  $\alpha^4 + 1$  dans la base  $\mathcal{B}$ .
- 10) Dans l'anneau des polynômes  $K[T]$ , posons

$$g = T^3 + T + 1.$$

On rappelle qu'il existe un corps fini contenant  $K$  dans lequel  $g$  a une racine  $\beta$ .

- 10.1) Que vaut  $\beta^7$  ?
  - 10.2) En déduire que  $g$  est irréductible dans  $K[T]$ .
  - 11) Posons  $L = K[T]/(g)$ .
    - 11.1) Quel est le cardinal  $q$  du corps  $L$  ?
    - 11.2) En utilisant les questions 6 et 10.1, déterminer la décomposition de  $q - 1$  en produit de nombres premiers.
    - 11.3) Quel est le nombre de générateurs de  $L^*$  ?
-