# Examen du 3 mai 2016

Aucun document n'est autorisé.

**Exercice 1** - (8 points) **QCM.** Une seule réponse parmi les 5 choix possibles (A,B,C,D ou E) est correcte. Il suffit d'indiquer la lettre pour chaque question ; aucun argument/justification/calcul n'est demandé.

Barème : réponse correcte +1 point, réponse fausse -0,5 point.

1. Le nombre de générateurs du groupe $(\mathbb{Z}/120\mathbb{Z}, +)$ est

   A : 1   B : 12   C : 32   D : 119   E : 120

2. Le nombre de générateurs du groupe des inversibles $((\mathbb{Z}/63\mathbb{Z})^*, .)$ est

   A : 1   B : 30   C : 31   D : 62   E : 63

3. L'ordre du groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}$ est

   A : 1   B : 2   C : 3   D : 6   E : $\infty$

4. L'ordre de la classe $\overline{2}$ dans le groupe $((\mathbb{Z}/17\mathbb{Z})^*, .)$ est

   A : 2   B : 4   C : 8   D : 16   E : 17

5. Soient $p, q, r$ trois nombres premiers distincts. Le nombre de diviseurs positifs du produit $pqr$ est

   A : 1   B : 3   C : 8   D : 16   E : ce nombre dépend de $p, q, r$

6. Le reste de la division euclidienne par 17 de $16! = 16 \cdot 15 \cdot 14 \cdots 3 \cdot 2$ est

   A : 0   B : 1   C : 3   D : 8   E : 16

   On considère le corps fini $K = \mathbb{F}_2[X]/X^3 + X + 1$ et on note $\alpha \in K$ la classe résiduelle du polynôme $X \in \mathbb{F}_2[X]$.

7. L'inverse de $\alpha$ dans le groupe multiplicatif $(K^*, .)$ est

   A : $\alpha$   B : $-\alpha$   C : $\alpha + 1$   D : $\alpha^2 + 1$   E : $\alpha$ n'admet pas d'inverse

8. L'ordre de $\alpha$ dans le groupe multiplicatif $(K^*, .)$ est

   A : 1   B : 2   C : 3   D : 7   E : 8

**Exercice 2** - (4 points) **Exemples.** Donner un exemple de

1. un nombre ayant exactement 3 diviseurs distincts positifs.
2. un polynôme de degré $\geq 1$ à coefficients dans $\mathbb{F}_3$ n'ayant pas de racines dans $\mathbb{F}_3$.
3. un homomorphisme de groupe injectif et non-surjectif.

4. deux entiers $a$ et $n$ avec $n \geq 2$ tels que $a^{\varphi(n)+1}$ n'est pas congru à $a$ modulo $n$.

**Exercice 3** - (4 points) **Fonction d'Euler.**

1. Donner la définition de la fonction d'Euler $\varphi(n)$ pour un entier positif $n$.
2. Déterminer l'ordre de la classe $\overline{-1}$ dans le groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^*$ pour un entier $n \geq 3$.
3. Déduire de la question précédente que $\varphi(n)$ est pair si $n \geq 3$.
4. En utilisant des résultats du cours, montrer que pour $n$ impair $\varphi(2n) = \varphi(n)$.

**Exercice 4** - (4 points) **Congruence.**
Calculer le reste de la division euclidienne par 11 du nombre

$$5^{10^{5^{10^5}}} + 10^{5^{10^{5^{10}}}}.$$