Examen – Mercredi 3 avril 2019 – 13h45 - 16h45

Tous les documents sont autorisés, mais l'utilisation d'internet est interdite. La clarté et la précision de la rédaction seront prises en compte très significativement. En particulier, les calculs faits avec `sage` doivent être justifiés, commentés et vérifiés. Les notations de l'énoncé doivent être suivies scrupuleusement.

Au début de l'examen :

— créer une nouvelle feuille de calcul `sage` en lui donnant comme nom le numéro d'anonymat figurant sur la copie d'examen.

À la fin de l'examen :

— créer un nouveau dossier dans le dossier personnel et donner à ce dossier comme nom le numéro d'anonymat figurant sur la copie d'examen,

— mettre dans ce dossier votre feuille de calcul (au format .ipynb),

— lancer un terminal (différent de celui avec lequel vous avez lancé `sage`) et taper la commande :

`copieexam` votre numéro d'anonymat

Le script affiche alors soit un message d'erreur soit le nouveau contenu déposé.

Exercice 1 (Les questions de cet exercice sont indépendantes).

1. Avec `sage`, calculer $3^{2^{32}}$ modulo $2^{32}+1$ (c'est le cinquième nombre de Fermat). Expliquer comment en déduire que $2^{32}+1$ n'est pas un nombre premier. Vérifier avec `sage` que $2^{32}+1$ n'est pas premier.
2. Soit $\xi = \mathrm{e}^{\frac{2i\pi}{3}}$, qui est l'une des deux racines du polynôme $P(X) = X^2 + X + 1$. Calculer l'inverse de la classe de $X^7 + 3$ dans $\mathbb{Q}[X]/(P)$ puis simplifier la fraction
$$\frac{(\xi+1)^4}{\xi^7+3}.$$
On demande que le résultat soit sous la forme d'un polynôme de petit degré en ξ. On pourra utiliser `sage` pour effectuer des calculs mais on n'oubliera pas de justifier la pertinence de ces calculs.
3. Avec `sage`, vérifier que le polynôme $P(X) = X^3 + X + 5$ est irréductible dans $(\mathbb{Z}/13\mathbb{Z})[X]$. On construit un corps à 2197 éléments en posant $\mathbb{F}_{2197} = (\mathbb{Z}/13\mathbb{Z})[X]/(P)$. Sans utiliser `sage`, donner une racine de P dans $\mathbb{F}_{2197}$ puis expliquer, toujours théoriquement, comment trouver d'autres racines (on ne demande pas d'expliciter ces racines). Avec `sage`, factoriser P dans $\mathbb{F}_{2197}[X]$ et comparer à vos résultats théoriques.

Le sujet continue page suivante.

Exercice 2 (Théorème chinois)**.** On considère les polynômes $P_1 = X^2+1$, $P_2 = X^2+2$ et $P_3 = X^2+4$ de $(\mathbb{Z}/127\mathbb{Z})[X]$. On pose $P = P_1P_2P_3$.

1. Vérifier dans `sage` que les polynômes P_i sont deux à deux premiers entre eux et irréductibles pour $i \in \{1, 2, 3\}$.
2. Soit

$$\begin{array}{rccc} \psi : & (\mathbb{Z}/127\mathbb{Z})[X]/(P) & \longrightarrow & (\mathbb{Z}/127\mathbb{Z})[X]/(P_1) \times (\mathbb{Z}/127\mathbb{Z})[X]/(P_2) \times (\mathbb{Z}/127\mathbb{Z})[X]/(P_3) \\ & R \bmod P & \longmapsto & (R \bmod P_1,\ R \bmod P_2,\ R \bmod P_3)\,. \end{array}$$

   Justifier à l'aide du cours que ψ est un isomorphisme.
3. Dans `sage`, définir une fonction `Psi` qui envoie un polynôme $R \in (\mathbb{Z}/127\mathbb{Z})[X]$ sur une liste de représentants des trois composantes de $\psi(R \bmod P)$.
4. Donner une formule explicite pour ψ^{-1} (on pourra utiliser `sage` pour effectuer d'éventuels calculs). Dans `sage`, à l'aide de la formule précédente, écrire une fonction `PsiInv` qui envoie une liste `[R_1, R_2, R_3]` de trois polynômes à coefficients dans $\mathbb{Z}/127\mathbb{Z}$ sur un polynôme représentant $\psi^{-1}(R_1 \bmod P_1, R_2 \bmod P_2, R_3 \bmod P_3)$.
5. Calculer `PsiInv(Psi(S))` pour $S \in \{X^2+2, X^2, X^6+7X^4+15X^2+8\}$ et commenter.
6. Quelle est la nature de $(\mathbb{Z}/127\mathbb{Z})[X]/(P_i)$ pour $i \in \{1, 2, 3\}$?
7. Sans utiliser `sage` et en justifiant soigneusement, déterminer le nombre d'inversibles de l'anneau $(\mathbb{Z}/127\mathbb{Z})[X]/(P)$.

Exercice 3. Soit $p = 13$, et $n \geq 2$.

1. Combien y a-t-il d'inversibles dans $\mathbb{Z}/13^n\mathbb{Z}$?
2. Avec `sage`, trouver un élément $\overline{u}$ d'ordre 12 dans $(\mathbb{Z}/13\mathbb{Z})^\times$.

On note u un relevé de $\overline{u}$ à $\mathbb{Z}$, et pour $n \geq 1$, u_n la classe u dans $\mathbb{Z}/13^n\mathbb{Z}$. En particulier, $u_1 = \overline{u}$.

3. Montrer que si $n \geq 1$ et $(u_n)^k = 1$ dans $\mathbb{Z}/13^n\mathbb{Z}$, alors $(\overline{u})^k = 1$ dans $\mathbb{Z}/13\mathbb{Z}$. En déduire que l'ordre de u_n dans $(\mathbb{Z}/13^n\mathbb{Z})^\times$ est divisible par 12.
4. Montrer que pour tout $n \geq 1$, il existe un élément de $(\mathbb{Z}/13^n\mathbb{Z})^\times$ d'ordre 12. Vérifier avec `sage` cette affirmation pour $n = 2$ et $n = 3$.

Exercice 4 (Base multiplicative de $\mathbb{F}_{16}$)**.**

1. (a) Sans utilise `sage`, faire la liste des polynômes de degré 2 dans $\mathbb{F}_2[X]$. Déterminer (toujours sans utiliser `sage`) les polynômes irréductibles de la liste précédente.
   (b) En déduire sans utiliser `sage` que le polynôme $P(X) = X^4 + X^3 + 1$ est irréductible dans $\mathbb{F}_2[X]$.
   (c) Définir $\mathbb{F}_{16}$ dans `sage` comme $\mathbb{F}_2[X]/(P)$. On note dans ce qui suit u la classe de X dans $\mathbb{F}_{16}$.
2. (a) Quelle est la dimension de $\mathbb{F}_{16}$ comme $\mathbb{F}_2$-espace vectoriel ? Donner une base de cet espace vectoriel.
   (b) Quel est le cardinal de $\mathbb{F}_{16}^\times$?
   (c) Vérifier avec `sage` que le groupe multiplicatif $\mathbb{F}_{16}^\times$ est engendré par u.
3. On note G l'ensemble des racines du polynôme $X^5 - 1$ dans $\mathbb{F}_{16}$
   (a) Montrer que G est un sous-groupe de $\mathbb{F}_{16}^\times$.
   (b) Sans utiliser `sage` exprimer les éléments de G comme des puissances de u.
   (c) À l'aide de G, construire une base (x_1, x_2, x_3, x_4) de $\mathbb{F}_{16}$ en tant que $\mathbb{F}_2$-espace vectoriel, tel que tout produit x_ix_j soit égal à un autre x_k ou à 1. Dresser la table de multiplication de cette base, et expliquer son intérêt pour les calculs dans $\mathbb{F}_{16}$. On pourra utiliser `sage` pour effectuer d'éventuels calculs.