Examen – Mercredi 11 avril 2018 – 13h00 - 16h00

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 répertoire 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 (Constructions de base)**.**

1. Afficher la liste des nombres premiers inférieurs à 100 congrus à 2 modulo 3.
2. Calculer un inverse Q de $P = X^2 + 3X + 2$ dans $\mathbb{Q}[X]/(X^2+1)$, et vérifier le résultat.
3. Sans utiliser `sage`, décrire explicitement la construction d'un corps à 9 éléments, et expliquer comment écrire la liste de ses éléments, ainsi que les opérations d'addition et de multiplication.
4. Vérifier à l'aide de `sage` que $P = T^4 + T^3 + T^2 + 1$ est irréductible dans $\mathbb{F}_5[X]$. Sans l'aide de `sage`, donner deux racines de P dans $K = \mathbb{F}_5[X]/(P)$. Pour chacune de ces racines, donner un représentant de degré au plus 3 de sa classe d'équivalence.

Exercice 2 (Théorème chinois)**.** On considère les polynômes $P_i = X - i \in \mathbb{Q}[X]$, $i \in \{1,2,3\}$ et $P = P_1P_2P_3$.

1. Vérifier dans `sage` que les P_i sont premiers entre eux deux à deux.
2. Soit
$$\begin{array}{rccc} \psi: & \mathbb{Q}[X]/(P) & \longrightarrow & \mathbb{Q}[X]/(P_1) \times \mathbb{Q}[X]/(P_2) \times \mathbb{Q}[X]/(P_3) \\ & R \bmod P & \longmapsto & (R \bmod P_1,\ R \bmod P_2,\ R \bmod P_3)\,. \end{array}$$
Justifier à l'aide du cours que ψ est un isomorphisme et expliciter son inverse.
3. Dans `sage`, définir une fonction `Psi` qui envoie un polynôme $R \in \mathbb{Q}[X]$ sur une liste de représentants des trois composantes de $\psi(R \bmod P)$.
4. Dans `sage`, définir, sans utiliser `crt` ou `CRT_list`, une fonction `PsiInv` qui envoie une liste `[R_1, R_2, R_3]` de trois polynômes à coefficients rationnels 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 $S \in \{X+1, X^2, X^8\}$ et commenter.

Exercice 3 (Classe de 5 modulo 2^n)**.**

1. Pour n entier entre 3 et 30, dresser avec `sage` la liste des ordres de $k = 5$ dans le groupe multiplicatif $((\mathbb{Z}/2^n\mathbb{Z})^*, \times)$.
2. Proposer une formule générale pour l'ordre $\omega(5)$ de 5 dans le groupe multiplicatif $(\mathbb{Z}/2^n\mathbb{Z})^*$ (on demande une formule valable pour tout $n \geq 3$).
3. Montrer que pour tout $n \geq 3$, $5^{2^{n-3}} \equiv 2^{n-1} + 1 \bmod 2^n$. En déduire une preuve de la formule pour $\omega(5)$ devinée à la question précédente.

Exercice 4 (Polynômes primitifs sur $\mathbb{F}_p$)**.** On considère le polynôme de $\mathbb{F}_7[X]$ donné par $P(X) = X^3 + X + 6$.

1. En utilisant éventuellement `sage` pour calculer dans $\mathbb{F}_7$, mais néanmoins sans utiliser la commande `P.is_irreducible()`, montrer que P est un polynôme irréductible de $\mathbb{F}_7[X]$.
2. On pose $k = \mathbb{F}_7[X]/(P)$, et on note t_0 la classe d'équivalence de X dans k. Utiliser `sage` pour montrer que P a trois racines dans k, et les exprimer en fonction de t_0.
3. Quelle est l'action du morphisme de Frobenius F sur les 3 racines de P dans k ?
4. On note $\omega(t)$ l'ordre d'un élément de k non nul dans le groupe multiplicatif $(k^*, \times)$. Montrer que cette quantité est invariante par F : pour tout $t \in k^*$, $\omega(F(t)) = \omega(t)$.
5. Déduire de la question précédente que les racines de P dans k ont toutes le même ordre multiplicatif, qu'on notera $\omega(P)$. Utiliser `sage` pour le vérifier et calculer cet ordre.
6. On admet qu'un polynôme irréductible de degré n sur $\mathbb{F}_p[X]$ a toujours n racines dans $\mathbb{F}_{p^n}$, et qu'elles sont permutées cycliquement par l'action du morphisme de Frobenius. Trouver un polynôme P unitaire irréductible de degré 3 sur $\mathbb{F}_7$ qui est *primitif*, c'est-à-dire tel que chacune de ses racines est un générateur du groupe cyclique $((\mathbb{F}_{7^3})^*, \times)$.