Examen – 5 avril 2022 – 15h30-18h30

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.

1. Soit K un corps, et $a_1, \dots, a_n \in K$ deux à deux distincts.
   (a) Quel est le reste de P modulo $X - a_1$?
   (b) Expliquer pourquoi l'homorphisme $\psi : K[X] \to K[X]/(X - a_1) \times K[X]/(X - a_2) \times \cdots \times K[X]/(X - a_n)$ défini par
   $$\psi(P) = (P \bmod (X - a_1), \dots, P \bmod (X - a_n))$$
   est surjectif.
2. En déduire qu'il existe $P_0 \in \mathbb{F}_{17}[X]$ tel que $P_0(0) = -1$, $P_0(1) = 0$, $P_0(2) = 7$ et $P_0(3) = 5$.
3. Calculer un tel P_0 grâce à `sage`. Quel est le degré du polynôme que vous avez obtenu ?
4. On veut maintenant chercher une fraction rationnelle $r = p/q \in \mathbb{F}_{17}(X)$ telle que r soit définie en $0, 1, 2, 3$ et $r(0) = -1$, $r(1) = 0$, $r(2) = 7$ et $r(3) = 5$. On veut de plus que p soit de degré minimal.
   (a) On note $R = X(X - 1)(X - 2)(X - 3)$. Montrer que q doit être inversible dans l'anneau $A = \mathbb{F}_{17}[X]/(R)$.
   (b) Expliquer pourquoi il suffit de trouver p et q dans $\mathbb{F}_{17}[X]$ (avec p de degré minimal) tels que $p = P_0 q$ dans A.
   (c) Expliquer pourquoi p doit être multiple de $\operatorname{pgcd}(R, P_0)$. En déduire que $\deg(p) \geqslant 1$.
   (d) Grâce à l'algorithme d'Euclide, trouver une solution (p, q) avec $\deg(p) = 1$.

Exercice 2. Nombres pseudo-premiers de Perrin

On définit une suite à valeurs entières par $u_0 = 3$, $u_1 = 0$, $u_2 = 2$ et, pour tout $n \geqslant 3$,

$$u_{n+3} = u_n + u_{n+1}$$

1. Calculer, à l'aide de `sage`, les 30 premiers termes de la suite u_n.
2. En utilisant `sage`, vérifier que le polynôme $P = X^3 - X - 1$ a une unique racine réelle ρ et en donner une valeur approchée.
3. Calculer u_{10^6}.
4. Soit p un nombre premier.
   (a) Expliquer pourquoi il existe un corps fini k de caractéristique p sur lequel P est scindé.
   (b) On fixe un tel corps et on note α, β, γ les racines (pas forcément distinctes) de P dans k. Notons $\overline{u}_n$ l'image de u_n dans $\mathbb{Z}/p\mathbb{Z}$.
   Démontrer que, pour tout $n \geqslant 0$, on a dans k
   $$\overline{u}_n = \alpha^n + \beta^n + \gamma^n$$
   (c) En déduire que p divise u_p.
5. Grâce à `sage`, vérifier ce théorème pour tous les nombres premiers inférieurs à 10000.
6. Soit $n \in \mathbb{N}$. On veut pouvoir tester efficacement si $n|u_n$.
   (a) Soit $\overline{u}_k$ l'image de u_k dans $\mathbb{Z}/n\mathbb{Z}$. Ecrire une relation de récurrence vérifiée par la suite $(\overline{u}_k)$.
   (b) Vérifier que pour $1 < n < 10^4$ on a $n|u_n$ si et seulement si n est premier.
   (c) Soit $n = 271441$. Vérifier que n n'est pas premier, mais que $n|u_n$.

Exercice 3. Coniques sur un corps fini

Soit $p \geqslant 3$ un nombre premier, et $a, b, c, d, e, f \in \mathbb{F}_p$ des coefficients. On considère la conique

$$C_{a,b,c,d,e,f}(p) = \{(x, y) \in (\mathbb{F}_p)^2 \mid ax^2 + bxy + cy^2 + dx + ey + f = 0\}.$$

L'objectif de l'exercice est de calculer le cardinal $|C_{a,b,c,d,e,f}(p)|$ de la conique en fonction des coefficients a, b, c, d, e, f.

1. Écrire un programme `conic(p,a,b,c,d,e,f)` qui prend en argument un nombre premier p et 6 entiers a, b, c, d, e, f, et qui renvoie l'ensemble des paires d'entiers modulo p qui appartiennent à la conique $C(p)$. Combien d'éléments contient la conique $C_{1,1,1,1,1,1}(11)$?
2. On suppose dans toute la suite de l'exercice $b^2 - 4ac \neq 0 \bmod p$ (on dit que la conique est non dégénérée).
   L'objectif de cette question est de démontrer que pour toute conique $C_{a,b,c,d,e,f}$ non dégénérée, il existe a', c', d', e' dans $\mathbb{F}_p$ et un isomorphisme linéaire $\psi : (\mathbb{F}_p)^2 \to (\mathbb{F}_p)^2$ tels que :
   - $\psi(C_{a,b,c,d,e,f}(p)) = C_{a',0,c',d',e',f}(p)$,
   - $b^2 - 4ac = -4a'c'$ (conservation du discriminant).

   (a) Traiter le cas $a \neq 0$. On pourra utiliser la «forme canonique» d'un trinôme du second degré.
   (b) Traiter le cas $a = 0$ et $c \neq 0$.
   (c) Traiter le cas $a = c = 0$ (et donc $b \neq 0$).
3. En déduire que $|C_{a,b,c,d,e,f}(p)| = |C_{a',0,c',d',e',f}(p)|$. On se ramène ainsi au cas $b = 0$.
4. (a) En utilisant une translation bien choisie dans l'espace $(\mathbb{F}_p)^2$, montrer que si $ac \neq 0$, alors
   $$|C_{a,0,c,d,e,f}(p)| = \left| C_{a,0,c,0,0,f-\frac{d^2}{4a}-\frac{e^2}{4c}}(p) \right|.$$

(b) Illustrer ce résultat avec `sage` et $p = 11$, $a = c = f = 1$ et différentes valeurs de d, e et f.

Dans tout ce qui suit, on supposera donc $ac \neq 0$ et $b = d = e = 0$, et on notera $C_{a,0,c,0,0,f}(p) = C_{a,c,f}(p)$.

5. On suppose $f = 0$.

   (a) Rappeler la définition du symbole de Legendre $\left(\frac{a}{p}\right)$. Expliquer pourquoi on a $\left(\frac{ac}{p}\right) = \left(\frac{ac^{-1}}{p}\right)$.

   (b) Montrer que
   $$|C_{a,c,0}(p)| = \begin{cases} 2p-1 & \text{si } \left(\frac{-ac}{p}\right) = 1, \\ 1 & \text{si } \left(\frac{-ac}{p}\right) = -1. \end{cases}.$$

6. Illustrer la question précédente en vérifiant avec un programme `sage` la formule pour $p = 11$ et toutes valeurs $a, c \neq 0 \bmod p$.

7. On suppose $f \neq 0$. Vérifier que pour $p = 11$ et toutes valeurs $a, c, f \neq 0 \bmod p$, la formule suivante est vraie :
   $$|C_{a,c,f}(p)| = \begin{cases} p-1 & \text{si } \left(\frac{-ac}{p}\right) = 1, \\ p+1 & \text{si } \left(\frac{-ac}{p}\right) = -1. \end{cases}.$$

   On ne demande pas de démontrer cette formule dans le cas général.