Mathématiques pour l'informatique. L1 Informatique UE-22. Contrôle

Terminal - Session 1 (correction) - Mai 2026

Exercice. L'objectif de ce problème est d'étudier le comportement de certaines suites de nombres entiers, dites *pseudo-aléatoires*. Elles sont utilisées dans les fonctions `random` des langages de programmation. L'algorithme qui génère ces suites de nombres est le suivant :

On se donne deux entiers naturels a et n premiers entre eux avec $n \geqslant 2$ et une valeur initiale $x_0 \in \mathbb{Z}/n\mathbb{Z}$ appelée *graine*. On définit alors la suite $(x_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{Z}/n\mathbb{Z}$ par la récurrence :

$$\forall k \geqslant 0 \quad x_{k+1} := a\,x_k \pmod n \tag{♯}$$

On s'intéressera plus particulièrement au cas où n est un nombre premier.

1» Dans cette question seulement, $n = 5$ et $x_0 = 1$. Complétez les valeurs manquantes dans le tableau pour les différentes valeurs de $a \neq 0$:

a	x_0	x_1	x_2	x_3	x_4	x_5	x_6
1	1						
2	1	2	4				
3	1						
4	1						

Que constatez-vous ?

Réponse.

a	x_0	x_1	x_2	x_3	x_4	x_5	x_6
1	**1**	1	1	1	1	1	1
2	**1**	**2**	**4**	**3**	1	2	4
3	**1**	**3**	**4**	**2**	1	3	4
4	**1**	**4**	1	4	1	4	1

Apparemment, les suites sont périodiques avec des périodes différentes.

2» Démontrez la proposition suivante par récurrence

$$\forall k \in \mathbb{N} \quad x_k = a^k x_0 \pmod n. \tag{⋆}$$

en explicitant le prédicat P que vous utilisez.

Réponse. Le prédicat $P(k)$ est défini par « $x_k = a^k x_0 \pmod n$ ».

Initialisation. Comme $a^0 = 1$, $P(0)$ est vrai puisque $x_0 = a^0 x_0$.

Hérédité. Soit $k \in \mathbb{N}$, montrons que $P(k) \Rightarrow P(k+1)$.
On a $x_{k+1} = a\,x_k \pmod n$, mais l'hypothèse de récurrence $P(k)$ nous fournit $x_k = a^k x_0 \pmod n$, donc $x_{k+1} = a\,(a^k x_0) = a^{k+1}\,x_0 \pmod n$ et finalement $P(k+1)$ est vrai.

On en déduit la proposition (⋆).

3» Démontrez que pour tout indice $p > 0$ tel que $x_p = x_0$, la suite est périodique de période p, c'est-à-dire :

$$\forall k \in \mathbb{N} \quad x_{k+p} = x_k$$

Réponse. Soit $k \in \mathbb{N}$, d'après (⋆) démontré en Q2 :

$$\begin{aligned} x_{k+p} &= a^{k+p} x_0 \\ &= (a^k a^p) x_0 \\ &= a^k (a^p x_0) \\ &= a^k x_p \\ &= a^k x_0 \\ &= x_k \end{aligned}$$

On notera qu'il peut exister plusieurs périodes : si p est une période, alors $\ell\,p$ l'est aussi pour tout entier $\ell \geqslant 1$. On cherchera donc toujours la *plus petite* période.

4» Pour $n := 5$, quelle est la *plus petite* période p de la suite (♯) pour chacune des valeurs $a \neq 0$?

Réponse. Pour les valeurs $a := 1, 2, 3, 4$, la plus petite période est $p = 1, 4, 4, 2$ respectivement.

5» On rappelle que le sous-ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ forme un groupe pour la multiplication. Pour $n = 5$, vérifiez que ce groupe est monogène et donnez tous ses générateurs.

Réponse. Rappelons qu'un groupe est *monogène* s'il admet un générateur, c'est-à-dire un élément dont les puissances successives engendrent tout le groupe. Ici $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$ est d'ordre 4. Le tableau de la question 1 met en évidence que $\langle 2 \rangle = \{1, 2, 4, 3\} = (\mathbb{Z}/5\mathbb{Z})^\times$, donc le groupe est

monogène. Les générateurs sont $a = 2$ et $a = 3$ (les deux éléments de plus petite période 4).

6» Dans cette question $n = 13$ et a est premier avec n. Justifiez que $a^{12} \equiv 1 \pmod{13}$.

Réponse. D'après le petit théorème de Fermat, si p est un nombre premier et $(a, p) = 1$, alors $a^{p-1} \equiv 1 \pmod{p}$. Ici $p = 13$ est premier et $(a, 13) = 1$ par hypothèse, donc $a^{12} \equiv 1 \pmod{13}$.

7» Soit n un nombre premier quelconque, a est premier avec n et t le plus petit entier non-nul tel que

$$a^t \equiv 1 \pmod{n}$$

Montrez que $t \mid (n-1)$. En déduire que la plus petite période de la suite $(x_k)_{k\in\mathbb{N}}$ définie par (♯) est un diviseur de $n-1$.

Réponse. Comme t est le plus petit entier non-nul tel que $a^t \equiv 1 \pmod{n}$, le sous-groupe monogène engendré par a est $\langle a \rangle = \{1, a, a^2, \ldots, a^{t-1}\}$, qui est d'ordre t. D'après le théorème de Lagrange, l'ordre de tout sous-groupe divise l'ordre du groupe ambiant ; ici $|(\mathbb{Z}/n\mathbb{Z})^\times| = n-1$ puisque n est premier, donc $t \mid (n-1)$.

On en déduit que la plus petite période de la suite $(x_k)_{k\in\mathbb{N}}$ divise $(n-1)$: en effet, d'après $(\star)$, $x_k = a^k x_0 \pmod{n}$, donc la suite revient à x_0 dès que $a^t \equiv 1$, et le plus petit tel t est exactement la plus petite période.

8» Si $(x_k)_{k\in\mathbb{N}}$ est une suite périodique de plus petite période p, le p-uplet $(x_0, x_1, \ldots, x_{p-1})$ constitue le *motif* de cette suite. Écrire une fonction *Python* `motif(n,a,x0)` qui renvoie sous forme de `tuple`, le motif de la suite $(x_k)_{k\in\mathbb{N}}$ définie en (♯) pour un entier $n \geqslant 2$, un entier a premier avec n et une graine x_0 fixés.

Réponse.

```
def motif(n, a, x0):
    T = (x0,)
    x = (a * x0) % n
    while x != x0:
        T += (x,)
        x = (a * x) % n
    return T
```

9» Soit a et n deux entiers naturels premiers entre eux avec $n \geqslant 2$. Montrez que l'application $f : x \mapsto ax$ est une permutation des éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$. Quelle autre condition doit satisfaire a pour que cette permutation soit de type $(n-1)$?

Réponse. Montrons que f est une bijection. Soit x et x' deux éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ tels que $f(x) = f(x')$. Alors $ax \equiv ax' \pmod{n}$, mais a étant premier avec n, il admet un inverse a^{-1} modulo n et

$$\begin{aligned} a^{-1}(ax) &= a^{-1}(ax') \\ (a^{-1}a)x &= (a^{-1}a)x' \quad \text{(associativité du produit)} \\ x &= x' \quad \text{(symétriques puis neutre)} \end{aligned}$$

Par conséquent f est injective. Elle est également surjective puisque toute application injective d'un ensemble fini dans un ensemble fini de même cardinal est surjective.

Si la permutation est de type $(n-1)$, cela signifie qu'elle se décompose en un unique cycle de longueur $n-1$ et par conséquent que tous les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ apparaissent dans ce cycle. Autrement dit, a est un élément d'ordre $n-1$ et donc un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$.

10» Soit $n = 5$ et $a = 3$. Soit x_0 une graine choisie au hasard dans $\{1, 2, 3, 4\}$ selon la loi uniforme. Calculez la loi de probabilité de la v.a.d. x_1. En déduire par récurrence que la v.a.d. x_k est uniformément distribuée sur $\{1, 2, 3, 4\}$ pour tout $k \geqslant 0$.

Réponse. On considère le prédicat $P(k)$ est « x_k est uniformément distribuée sur $\{1, 2, 3, 4\}$ ».

Initialisation. Par hypothèse, x_0 est uniforme sur $\{1, 2, 3, 4\}$, donc $P(0)$ est vrai.

Hérédité. Supposons $P(k)$ vrai, c'est-à-dire $\mathbb{P}(x_k = i) = \frac{1}{4}$ pour tout $i \in \{1, 2, 3, 4\}$. D'après la question précédente, l'application $x \mapsto 3x \bmod 5$ est une bijection de $(\mathbb{Z}/5\mathbb{Z})^\times$. Donc pour tout $j \in \{1, 2, 3, 4\}$, il existe un unique $i \in \{1, 2, 3, 4\}$ tel que $3i \equiv j \pmod{5}$, et

$$\mathbb{P}[x_{k+1} = j] = \mathbb{P}[3x_k = j] = \mathbb{P}[x_k = i] = \frac{1}{4}.$$

Ainsi $P(k+1)$ est vrai.

On conclut que x_k est uniforme sur $\{1, 2, 3, 4\}$ pour tout $k \geqslant 0$.