Informatique tronc commun
Devoir n° 3 – Partie sur machine

16 mars 2019

Durée : 60 minutes, documents et internet interdits.

1. **Lisez attentivement tout l'énoncé avant de commencer.**
2. Ce devoir est à réaliser seul, en utilisant Python 3.
3. Nous vous conseillons de commencer par créer un dossier au nom du DS dans le répertoire dédié à l'informatique de votre compte.
4. Nous vous rappelons qu'il est possible d'obtenir de l'aide dans l'interpréteur d'idle en tapant `help(nom_fonction)`.
5. Vous inscrirez vos réponses sur la feuille réponse fournie. Attention : lisez attentivement le paragraphe suivant.

Fonctionnement du devoir

Vos réponses dépendent d'un paramètre α, unique pour chaque étudiant, qui vous est donné en haut de votre fiche réponse. Notez-le bien !

Dans ce devoir, on notera $a\%b$ le reste de la division euclidienne de a par b.

Dans ce devoir, pour deux entiers a et b, on notera $[\![a;b[\![$ l'ensemble des entiers consécutifs allant de a (inclu) à b (exclu), c'est-à-dire que

$$[\![a;b[\![= \{a, a+1, \ldots, b-1\}.$$

Lorsque vous donnerez un résultat flottant, vous écrirez juste ses huit premières décimales.

Vous trouverez en annexe les réponses pour le paramètre $\alpha = 1$, utilisez-les pour vérifier la correction de vos algorithmes.

Lecture et traitement de fichier

Vous trouverez un fichier `frequences.txt` ainsi qu'un fichier `texte_`α`.txt` sur le site de classe ainsi qu'à l'adresse suivante (où `X` est à remplacer par `1` ou `2` et où α est à remplacer par votre numéro) :

$\sim$`/groupes/mpsX/données/d03s/frequences.txt`
$\sim$`/groupes/mpsX/données/d03s/texte_`α`.txt`

Le fichier sur lequel vous allez travailler a été chiffré en utilisant le chiffre de César. C'est un code par décalage très simple, qui fonctionne avec une clef $c \in [\![0, 26[\![$. En numérotant les lettres de 0 (lettre `a`) à 25 (lettre `z`), chaque lettre de numéro r est remplacée par la lettre de numéro $(r+c)\%26$.

Par exemple, si la clef est 2 (lettre `c`), le `a` est transformé en `c`, le `b` en `d`, ..., le `x` en `z`, le `y` en `a` et le `z` en `b`.

Indication : dans cet exercice, vous pourrez introduire `alphabet="abcdefghijklmnopqrstuvwxyz"`. Ainsi, si $i \in [\![0, 26[\![$, `alphabet[`i`]` sera la lettre n° i.

Q1 Appliquez la tranformation de clef 24 (lettre `y`) à votre texte. Quelle est le $(\alpha+50)^{\text{e}}$ mot de ce nouveau texte (on numérote à partir de zéro) ?

Pour déchiffrer un texte chiffré avec la clef c, il suffit d'appliquer la tranformation de clef $(26-c)\%26$. Cette dernière clef sera appelée *clef de déchiffrement* du texte. Par exemple, si la clef de chiffrement est 3 (lettre `d`), alors la clef de déchiffrement sera 23 (lettre `x`).

La cryptanalyse du chiffre de César, c'est-à-dire l'obtention de la clef à partir du texte chiffré, peut se faire par analyse de fréquences.

La fréquence d'une lettre dans un texte est le rapport entre le nombre d'occurences dans ce texte de cette lettre et le nombre total de lettres du texte.

Q2 Quelle est la fréquence de la lettre `e` dans votre texte chiffré ?

Pour comparer deux tableaux de fréquences de lettres $t = [t_0, \ldots, t_{25}]$ et $u = [u_0, \ldots, u_{25}]$, on utilise la distance

$$d(t, u) = \sum_{k=0}^{25} (t_k - u_k)^2.$$

Le fichier `frequences.txt` contient une liste de fréquences des lettres, que l'on supposera être celle du français. Vous le retrouverez dans le tableau 1.

Lettre	a	b	c	d	e	f	g	h	i
Fréquence	0,0840	0,0106	0,0303	0,0418	0,1726	0,0112	0,0127	0,0092	0,0734
Lettre	j	k	l	m	n	o	p	q	r
Fréquence	0,0031	0,0005	0,0601	0,0296	0,0713	0,0526	0,0301	0,0099	0,0655
Lettre	s	t	u	v	w	x	y	z	
Fréquence	0,0808	0,0707	0,0574	0,0132	0,0004	0,0045	0,0030	0,0012	

TABLE 1 – Tableau des fréquences des lettres en français

Q3 Quelle est la distance entre le tableau des fréquences des lettres de votre texte chiffré et celui des fréquences données dans le fichier `frequences.txt` ?

L'algorithme de déchiffrement est le suivant : pour chaque clef $c \in [\![0, 26[\![$, on applique le code de César de clef c au texte (ce qui donne un second texte), puis l'on calcule le tableau des fréquences des lettres de ce second texte, et enfin l'on calcule la distance entre ce tableau et celui donné par le fichier `frequences.txt`.

On sélectionne alors la clef qui minimise les distances calculées ci-dessus.

Q4 Quelle est la clef de déchiffrement de votre texte ?

Q5 Quelle est le $(\alpha + 100)^{\mathrm{e}}$ mot du texte déchiffré (on numérote à partir de zéro) ?

Méthodes numériques

On considère l'équation différentielle $y' + (t+1)^2 y = \mathrm{e}^{\arctan t}$, avec la condition initiale $y(0) = y_0 = \arctan \alpha$, et on note f la solution de cette équation différentielle sur $\mathbb{R}^+$ (on admettra son existence et son unicité). On rappelle que la fonction arctan est donnée par la fonction `atan` du module `math`.

Q6 En prenant pour pas $h = \frac{1}{10}$, donner la valeur approchée de $f(1)$ obtenue par la méthode d'Euler appliquée à ce problème de Cauchy.

On considère l'équation différentielle $y'' + (t+1)^2 y' + y = \mathrm{e}^t$, avec les conditions initiales $y(0) = y_0 = \arctan \alpha$ et $y'(0) = \sin \alpha$, et on note g la solution de cette équation différentielle sur $\mathbb{R}^+$ (on admettra son existence et son unicité).

Q7 En prenant pour pas $h = \frac{1}{10}$, donner les valeurs approchées de $g(1)$ et de $g'(1)$ obtenues par la méthode d'Euler appliquée à ce problème de Cauchy.

Soit

$$I = \int_4^5 \frac{\sin t}{t} \mathrm{d}t.$$

Q8 Donner la valeur approchée de I obtenue par la méthode des trapèzes avec $5 + \alpha$ trapèzes.

Un exercice.

Conseil : n'attaquez cet exercice que si vous avez répondu aux questions précédentes.

On admet que pour tout entier $n \geq 1$ il existe une unique suite $a_1, \ldots, a_p$ vérifiant :

— $n = \displaystyle\sum_{k=1}^{p} a_k \times k!$

— $a_p \neq 0$ et $\forall k \in [\![1, p]\!]$, $0 \leq a_k \leq k$.

On appellera *écriture en base factorielle* de l'entier n la chaîne $a_1 - a_2 - \cdots - a_p$.

Par exemple, $42 = 0 \times 1! + 0 \times 2! + 3 \times 3! + 1 \times 4!$, l'écriture de 42 en base factorielle est donc $0 - 0 - 3 - 1$.

Q9 Donner l'écriture en base factorielle de $\alpha^3 + \alpha^2 + \alpha + 10^5$.

Informatique tronc commun
Devoir n° 3 – Partie sur machine

Fiche de test

$$\boxed{\alpha = \mathbf{1}}$$

R1 :	`oktrhdtqr`
R2 :	0,032748538
R3 :	0,081302026
R4 :	*Nous n'allions quand même pas vous la donner*
R5 :	`virgule`
R6 :	0,644571871
R7 – $g(1)$:	1,336829746
R7 – $g'(1)$:	0,328788754
R8 :	-0,207782868
R9 :	1-0-3-1-5-5-3-2