

NOM : Hanon Ymous  
(000000)  
Place : 0

#0000



## Information, Calcul et Communication (SMA/SPH) Examen

12 janvier 2021

### INSTRUCTIONS (à lire attentivement)

**IMPORTANT!** Veuillez suivre les instructions suivantes à la lettre sous peine de voir votre examen annulé dans le cas contraire.

1. Vous disposez de trois heures pour faire cet examen (16h15 – 19h15).
2. Vous devez **écrire à l'encre noire ou bleu foncée**, pas de crayon ni d'autre couleur. N'utilisez **pas non plus de stylo effaçable** (perte de l'information à la chaleur).
3. Vous avez droit à toute documentation papier.  
En revanche, vous ne pouvez pas utiliser d'ordinateur personnel, ni de téléphone portable, ni aucun autre matériel électronique.
4. Répondez aux questions directement sur la donnée.  
Ne joignez aucune feuilles supplémentaires; **seul ce document sera corrigé**.
5. Lisez attentivement et *complètement* les questions de façon à ne faire que ce qui vous est demandé. Si l'énoncé ne vous paraît pas clair, ou si vous avez un doute, demandez des précisions à l'un des assistants.
6. L'examen comporte 8 exercices indépendants sur 12 pages, qui peuvent être traités dans n'importe quel ordre, mais qui ne rapportent pas la même chose (les points sont indiqués, le total est de 150 points).  
Tous les exercices comptent pour la note finale.



## Question 1 – Un p’tit algo [10 points]

Un étudiant a écrit l’algorithme suivant :

<b>Machin</b>
entrée : $a$ , entier strictement positif sortie : ???
$b \leftarrow 0$ $c \leftarrow 1$ $d \leftarrow 0$ <b>Tant que</b> $c < a$ $d \leftarrow d + 1$ <b>Si</b> $d$ est un multiple de 7 ou de 11 $b \leftarrow b + d$ $c \leftarrow c + 1$ <b>Sortir</b> : $b$

① [4 points] Quelle valeur sort cet algorithme pour  $a = 7$ ? Expliquez cette valeur en une phrase/formule.

② [6 points] Ecrire une fonction C++ qui implémente cet algorithme.

Réponse ① : \_\_\_\_\_

Réponse ② :



---

## Question 2 – Ecriture d’algorithmes [41 points]

① [15 points] Ecrivez une **fonction C++** qui effectue la fusion triée de deux listes triées.

Par exemple, si en entrée on a les listes  $L_1 = (-5, 1, 4, 18)$  et  $L_2 = (-12, -6, 8, 33, 107)$ , alors en sortie on aura la liste  $(-12, -6, -5, 1, 4, 8, 18, 33, 107)$ .

② [5 points] Quelle est la complexité de l’algorithme correspondant à votre fonction C++ ?

**Réponses :**

suite au dos ➞



---

③ [21 points] Ecrivez une **fonction C++ *récursive*** qui, prenant en entrée deux listes quelconques (y compris vides), effectue leur fusion alternée, « poussée à droite » en cas d'éléments excédentaires dans une des deux listes.

Par exemple :

- si en entrée on a les deux listes  $L_1 = (1, 2, 3)$  et  $L_2 = (-11, -22, -33)$  (dans cet ordre), alors en sortie on aura la liste  $(1, -11, 2, -22, 3, -33)$  ;
- si en entrée on a les deux listes  $L_1 = (1, 2, 3, 4)$  et  $L_2 = (-11, -22, -33)$  (dans cet ordre ;  $L_1$  plus grande), alors en sortie on aura la liste  $(1, 2, -11, 3, -22, 4, -33)$  ;
- par contre, si en entrée on a les deux listes dans l'autre ordre :  $L_1 = (-11, -22, -33)$  et  $L_2 = (1, 2, 3, 4)$ , alors en sortie on aura la liste  $(1, -11, 2, -22, 3, -33, 4)$  ;
- encore deux exemples si nécessaire : si en entrée on a les deux listes :  $L_1 = (-11, -22)$  et  $L_2 = (1, 2, 3, 4, 5, 6)$ , alors en sortie on aura la liste  $(1, 2, 3, 4, -11, 5, -22, 6)$  ;
- enfin, si en entrée on a les deux listes dans l'autre ordre :  $L_1 = (1, 2, 3, 4, 5, 6)$  et  $L_2 = (-11, -22)$ , alors en sortie on aura la liste  $(1, 2, 3, 4, 5, -11, 6, -22)$ .

**Réponse :**



---

**Question 3 – Compression de génome [20 points]**

Une entreprise de séquençage de génome veut stocker efficacement ses résultats sur disque. Les séquences à coder n'utilisent que 5 lettres : A, C, G, T et l'espace (pour dire « inconnu » ou « coupé », notée ici  $\square$ ).

Par exemple (20 lettres) :

T A G C G  $\square$  C G C C T A C G  $\square$  C A T G T

① [7 points] Quelle est l'entropie (en bit) de la séquence ci-dessus ?

Donnez votre réponse sous la forme  $a + b \log_2(3) + c \log_2(5)$  en exprimant la valeur de  $a$ , de  $b$  et de  $c$  sous forme de fraction irréductible :

$a =$

$b =$

$c =$

et **justifiez** votre réponse :

② a) [5 points] Proposez un code de Huffman binaire pour cette séquence. Donnez ici votre arbre de codage :

b) [1.5 points] Si vous codez cette séquence avec votre code, combien avez-vous de bits au total ?

c) [2 points] Quel taux de compression obtenez vous par rapport à un codage binaire naïf ? Justifiez votre réponse.

suite au dos 



③ [4.5 points] La vraie entropie de leurs séquences est de 2.5 bit. Quelle taille de disque (en Gio) doivent ils prévoir (environ) pour les 10 prochaines années sachant qu'ils produisent en moyenne par année  $10^5$  séquences de longueur moyenne  $10^9$  caractères ?

**Justifiez** votre réponse.

## Question 4 – Complexité [15 points]

Considérez le programme suivant :

```
unsigned int f(unsigned int i, unsigned int j)
{
    if (i <= j) return j;
    unsigned int a(2*i - j);
    while (i > j) {
        a += 3;
        --i;
    }
    return a + f(j, a) + 2;
}
```

① [3 points] Calculer  $f(6, 4)$ .

② [12 points] Quelle est la complexité de l'algorithme implémenté par  $f$  ?

**Justifier** votre réponse.

Réponses :



---

**Question 5 – RSA [13 points]**

Nous considérons utiliser RSA avec  $p = 7$  et  $q = 13$  (et donc  $n = 91$ ).

① [3.5 points] Dans ce cadre, est-ce que les valeurs suivantes sont des valeurs possibles pour notre clé privée  $d$ ? Justifiez à chaque fois votre réponse.

$d = 15$  :

$d = 35$  :

$d = 85$  :

② [2 points] Nous choisissons finalement comme clé privée  $d = 29$ . Vérifiez alors, en explicitant ici vos calculs, que notre clé publique est  $e = 5$ .

**Justification :**

③ [3 points] Quelqu'un veut nous envoyer le message correspondant à la valeur (décimale) 10. Quel message (valeur décimale) nous envoie-t-il pour assurer la confidentialité de ce message? Justifiez pleinement votre réponse (en explicitant tous les calculs si nécessaire).

**Réponse et justification :**

④ [3 points] Nous décidons de changer de clé et utilisons maintenant la clé publique  $(5'239, 1'863'227)$  avec la clé privée 11'719.

Supposons que nous recevions le message crypté suivant, en binaire : 11011110.

Quel message nous a-t-on envoyé?

Donnez ici simplement la formule (en décimal), *sans* calculer explicitement la valeur.

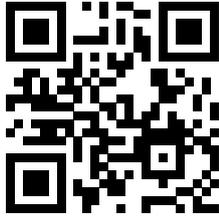
**Réponse :**

⑤ [1.5 points] Toujours avec la paire de clés  $(5'239, 1'863'227)$  et 11'719, supposons que nous voulions signer un message correspondant à la valeur (décimale) 12'345.

Quelle signature utilisons nous? (uniquement la signature, pour responsabilisation, *sans* souci de confidentialité ici).

Donnez ici simplement la formule (en décimal), *sans* calculer explicitement la valeur.

**Réponse :**



## Question 6 – La bonne droite [25 points]

On s'intéresse dans cet exercice à écrire un programme C++ pour faire passer une droite au mieux au milieu d'un nuage de points dans le plan.

① [1 point] Commencez par écrire ici un type C++, nommé `Point` permettant de modéliser un point dans le plan (représenté par deux nombres réels  $x$  et  $y$ ).

② [1 point] Écrivez ensuite ici un type C++, nommé `Line` permettant de modéliser une droite d'équation  $y = ax + b$  par ses deux coefficients : il suffit simplement de représenter  $a$  et  $b$ .

③ [8 points] On veut maintenant écrire une fonction C++ `fit()` qui reçoit en entrée une liste de  $n$  points et qui donne en sortie les paramètres  $a$  et  $b$  de la droite d'équation  $y = ax + b$  qui passe « au mieux » au milieu de cet ensemble de points.

Si l'on note  $x_i$  et  $y_i$  les coordonnées du point  $P_i$  de la liste ( $i$  de 1 à  $n$ ), les coefficients  $a$  et  $b$  de cette droite sont déterminés comme suit ( $b$  dépend de  $a$ ) :

$$a = \frac{\left(\sum_{i=1}^n x_i y_i\right) - \frac{1}{n} \left(\sum_{i=1}^n x_i\right) \left(\sum_{i=1}^n y_i\right)}{\left(\sum_{i=1}^n x_i^2\right) - \frac{1}{n} \left(\sum_{i=1}^n x_i\right)^2} \quad b = \frac{1}{n} \left( \left(\sum_{i=1}^n y_i\right) - a \left(\sum_{i=1}^n x_i\right) \right)$$

Écrivez ici le code C++ de la fonction `fit()`. Celle-ci ne doit contenir qu'une seule boucle.



Question 6

④ [1 point] Ecrivez une fonction C++ `line_value()` qui prend en paramètres une `Line` et un nombre réel  $x$  et retourne la valeur  $y = a x + b$  obtenue à partir de  $x$  et des coefficients de la droite passée en argument.

⑤ [5 points] Ecrivez une fonction C++ `mse()` qui prend en paramètres une `Line (a, b)` et un ensemble de points et qui calcule l'écart entre la droite et l'ensemble de points suivant la formule :

$$\text{MSE} = \frac{1}{n} \sum_{i=1}^n (y_i - (a x_i + b))^2$$

(où  $x_i$  et  $y_i$  sont les coordonnées du point  $P_i$  de la liste ; avec  $i$  de 1 à  $n$ ).

⑥ [9 points] Pour finir, on souhaite vérifier empiriquement avec du code C++ que la droite calculée en ③ est celle qui minimise l'écart (tel que calculé en ⑤).

Ecrire pour cela une fonction C++ `check_best_fit()` qui prend en paramètres une liste de points, un nombre réel  $\varepsilon$  et un entier  $m$ , et qui :

1. calcule la droite obtenue par `fit()` ; appelons  $\hat{a}$  et  $\hat{b}$  ses paramètres ;
2. calcule et affiche l'écart (fonction `mse()`) entre l'ensemble des points et chacune des  $(2m + 1)^2$  droites définies comme suit (suite et exemple au dos) :

suite au dos 



- 
- a) le paramètre de pente  $a$  de ces droites variera entre  $(\hat{a} - m \varepsilon)$  et  $(\hat{a} + m \varepsilon)$  par pas de  $\varepsilon$  (exemple ci-dessous);
- b) et le paramètre d'ordonnée à l'origine  $b$  de ces droites variera entre  $(\hat{b} - m \varepsilon)$  et  $(\hat{b} + m \varepsilon)$ , également par pas de  $\varepsilon$ .

Par exemple, avec  $\varepsilon = 0.1$  et  $m = 2$ , la fonction `check_best_fit()` testera les 25 droites suivantes : toutes les droites  $y = a x + b$  avec  $a$  parmi  $\{\hat{a} - 0.2, \hat{a} - 0.1, \hat{a}, \hat{a} + 0.1, \hat{a} + 0.2\}$  et  $b$  parmi  $\{\hat{b} - 0.2, \hat{b} - 0.1, \hat{b}, \hat{b} + 0.1, \hat{b} + 0.2\}$ . A noter donc que la droite calculée par `fit()` est testée au milieu de toutes ces droites.

Vous pouvez faire l'affichage comme vous voulez ; par exemple, afficher sur chaque ligne le  $a$ , le  $b$  puis l'écart (`mse()`) trouvé.

**Code de la fonction `check_best_fit()` :**



Question 7

**Question 7 – Mal aux sinus ? [16 points]**

① [9 points] Soit  $f$  une fonction de  $\mathbb{R}$  dans  $\mathbb{R}$  définie par

$$f(t) = \sum_{m \in \mathbb{Z}} a_m \operatorname{sinc}(35t - m)$$

où  $\operatorname{sinc}(x) = \frac{\sin(\pi x)}{\pi x}$  et  $a_m = K_1 \sin\left(\frac{4\pi}{7}m\right) + K_2 \sin\left(\frac{11\pi}{6}m + \frac{\pi}{5}\right) + K_3 \sin\left(\frac{6\pi}{5}m + \frac{\pi}{3}\right) + K_4 \sin\left(\frac{\pi}{4}m + \frac{\pi}{3}\right)$ .

Proposez des valeurs  $K_1, K_2, K_3, K_4$  pour pouvoir écrire  $f(t)$  comme la somme de *deux* fonctions sinus, puis écrivez  $f(t)$  comme la somme de deux fonctions sinus :

$$K_1 = \quad K_2 = \quad K_3 = \quad K_4 =$$

$$f(t) =$$

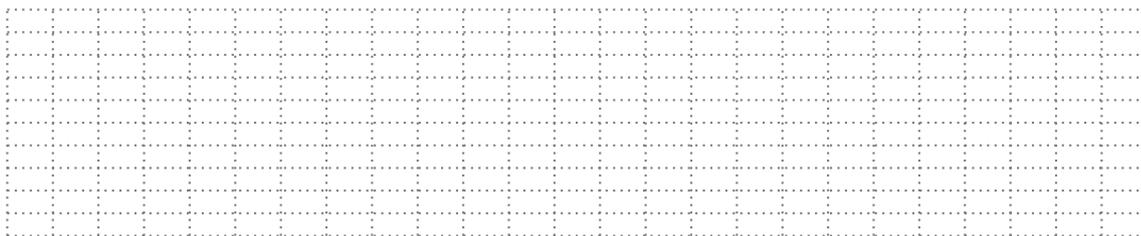
**Justifiez** votre réponse :

② On considère le signal

$$X(t) = 5 \sin\left(12\pi t + \frac{2\pi}{3}\right) + 3 \sin\left(24\pi t - \frac{\pi}{6}\right) + 7 \sin\left(8\pi t + \frac{3\pi}{4}\right) + 9 \sin\left(6\pi t - \frac{3\pi}{5}\right)$$

que l'on passe dans un filtre à moyenne mobile de fréquence de coupure  $f_c = 4$  Hz.

**a) [3 points]** Dessinez le spectre de  $X$  *avant* filtrage :



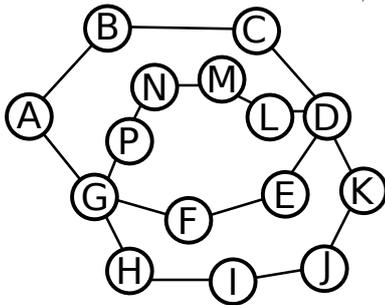
**b) [4 points]** Dessinez le spectre de  $\widehat{X}(t)$ , signal *après* filtrage, sachant que  $\operatorname{sinc}\left(\frac{3}{4}\right) \simeq 0.33$  et  $\operatorname{sinc}\left(\frac{3}{2}\right) \simeq -0.2$  :





### Question 8 – Des routes [10 points]

On considère le réseau TCP/IP suivant :



① [2 points] Donnez les lignes de la table de routage de A correspondant aux nœuds D, E, L et I :

② [1 point] Parmi les lignes précédentes (de la table de routage de A) lesquelles changent, et comment, si le nœud C « tombe » (c.-à-d. disparaît) ?

③ [7 points] On envoie un message de A vers K (avec C présent). Ce message est décomposé en 80 paquets. Sachant que

- chaque nœud met 8 ms à transmettre un paquet au nœud suivant ;
- on négligera tout autre temps ;
- en moyenne 1 paquet sur 5 est malheureusement perdu (au niveau 4) ;

quel est (en moyenne) le temps total de transmission de ce message ?

*Justifiez* votre réponse. **Note** : on pourra, si nécessaire, faire l'approximation  $9 \simeq 10$ .