Le Lièvre et la Tortue

Épreuve pratique d'algorithmique et de programmation
Concours commun des Écoles normales supérieures

Durée de l'épreuve: 3 heures 30 minutes

Juin/Juillet 2012

ATTENTION !

N'oubliez en aucun cas de recopier votre u_0
à l'emplacement prévu sur votre fiche réponse

Important.

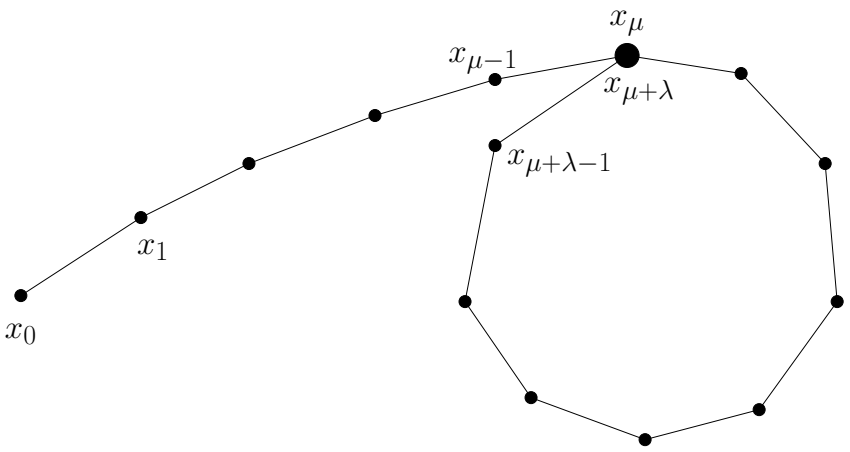
Sur votre table est indiqué un numéro u_0 qui servira d'entrée à vos programmes. Les réponses attendues sont généralement courtes et doivent être données sur la fiche réponse fournie à la fin du sujet. À la fin du sujet, vous trouverez en fait deux fiches réponses. La première est un exemple des réponses attendues pour un $\widetilde{u_0}$ particulier (précisé sur cette même fiche et que nous notons avec un tilde pour éviter toute confusion!). Cette fiche est destinée à vous aider à vérifier le résultat de vos programmes en les testant avec $\widetilde{u_0}$ au lieu de u_0. Vous indiquerez vos réponses (correspondant à votre u_0) sur la seconde et vous la remettrez à l'examinateur à la fin de l'épreuve.

En ce qui concerne la partie orale de l'examen, lorsque la description d'un algorithme est demandée, vous devez présenter son fonctionnement de façon schématique, courte et précise. Vous ne devez en aucun cas recopier le code de vos procédures!
Quand on demande la complexité en temps ou en mémoire d'un algorithme en fonction d'un paramètre n, on demande l'ordre de grandeur en fonction du paramètre, par exemple: $O(n^2)$, $O(n \log n)$,...
Il est recommandé de commencer par lancer vos programmes sur de petites valeurs des paramètres et de ***tester vos programmes sur des petits exemples que vous aurez résolus préalablement à la main ou bien à l'aide de la fiche réponse type fournie en annexe***. Enfin, il est recommandé de lire l'intégralité du sujet avant de commencer afin d'effectuer les bons choix de structures de données dès le début.

Pour toute fonction f qui envoie un ensemble fini E dans lui-même et $x_0 \in E$, considérons la suite des valeurs de la fonction itérée :

$$x_0, x_1 = f(x_0), x_2 = f(x_1), \ldots, x_i = f(x_{i-1}), \ldots$$

Cette suite va atteindre deux fois la même valeur, c'est-à-dire qu'il existe $i \neq j$ tel que $x_i = x_j$. Une fois que cette *collision* est obtenue, la suite des valeurs va répéter le cycle des valeurs de x_i à x_{j-1}. Nous nous intéressons au problème de rechercher un cycle dans la suite des valeurs d'une fonction itérée, c'est-à-dire de trouver i et j étant donnés f et x_0. Le graphe de la fonction représente la forme de la lettre grecque ρ. On notera $\mu = i$ la longueur de la pré-période et $\lambda = j - i$ la longueur du cycle.



1 Fonction aléatoire

Soit g la fonction définie par

$$g(x) = x^2 + 234 \bmod 32069.$$

Considérons $(u_k)_{k\geq 0}$ la suite d'entiers définie par les itérés de g :

$$u_k = \begin{cases} \text{votre } u_0 \quad (\textit{À reporter sur votre fiche réponse}) & \text{si } k = 0 \\ g(u_{k-1}) & k > 0. \end{cases}$$

On considère également la fonction f_p qui à l'entier x, associe l'entier $f_p(x)$ par la formule (1) où $v_0 = x \bmod p$ et $v_n = g(v_{n-1})$:

$$f_p(x) = \left(x + \sum_{k=1}^{k=28} \lfloor v_{29-k}/16035 \rfloor \cdot 2^{k-1} \right) \bmod 2^{28}. \tag{1}$$

Question 1 ***a)*** $(u_{10}, f_{u_{11}}(u_{10}))$ ***b)*** $(u_{20}, f_{u_{21}}(u_{20}))$ ***c)*** $(u_{50}, f_{u_{51}}(u_{50}))$.

Les parties 2, 3 et 4 sont indépendantes et il n'est pas nécessaire d'avoir programmé les questions de l'une pour aborder les questions des autres.

2 Recherche de cycle

Question 2 *Trouver la longueur de la pré-période et de la période de la fonction* $f'_p(x) = f_p(x) \bmod 10^6$ *itérée à partir de* x_0 *:*
a) $x_0 = u_{10}, p = u_{11}$ ***b)*** $x_0 = u_{20}, p = u_{21}$ ***c)*** $x_0 = u_{50}, p = u_{51}$.

Question à développer pendant l'oral : Quelle est la complexité de votre algorithme en temps et en espace ?

À partir de maintenant on s'intéressera aux itérés de la fonction f_p et non f'_p.

Soit la fonction

$$h_i(x) = \{j < i \mid x_j \bmod 10^6 = x \bmod 10^6\}$$

et considérons

$$i_0 \text{ le plus petit entier tel qu'il existe } j \in h_{i_0}(x_{i_0}) \text{ et } x_{i_0} = x_j.$$

Question 3 *Que valent* i_0 *et* j *pour les itérés de la fonction* f_p *et combien y a-t-il d'ensembles* $h_{i_0}(x)$ *non vides pour* $0 \leq x < 10^6$ *?*
a) $x_0 = u_{10}, p = u_{11}$ ***b)*** $x_0 = u_{20}, p = u_{21}$ ***c)*** $x_0 = u_{50}, p = u_{51}$.

Question à développer pendant l'oral : Quelle est la complexité de votre algorithme en temps et en espace ?

3 Recherche de cycle sans mémoire

3.1 Algorithme de Floyd

On peut éviter d'utiliser de la mémoire en employant l'algorithme de Floyd. Considérons la suite y_i définie par $y_0 = x_0$ et $y_i = f(f(y_{i-1}))$. On rappelle que $x_i = f(x_{i-1})$. L'algorithme calcule les valeurs de x_i et y_i et retourne la plus petite valeur $i > 0$ telle que $x_i = y_i$.

Question à développer pendant l'oral : Pourquoi x_i se trouve-t-il dans le cycle ? Expliquer pourquoi l'algorithme termine et pourquoi la valeur i correspond au plus petit multiple de la période supérieur à μ.

Question 4 *Donner les valeurs de* i *et* x_i *au moment où cet algorithme se termine pour la suite* $(x_k)_{k\geq 0}$ *des itérés de* f_p *à partir de* x_0 *:*
a) $x_0 = u_{10}, p = u_{11}$ ***b)*** $x_0 = u_{20}, p = u_{21}$ ***c)*** $x_0 = u_{50}, p = u_{51}$.

Question à développer pendant l'oral : Expliquer comment trouver la longueur du cycle à partir de i et x_i. Prouver que $x_{i+\mu} = x_\mu$ et en déduire comment trouver deux valeurs $x \neq x'$ telles que $f(x) = f(x')$.

Question 5 *Trouver les deux valeurs* $x \neq x'$ *qui sont des itérés de* f_p *à partir de* x_0 *telles que* $f_p(x) = f_p(x')$.
a) $x_0 = u_{10}, p = u_{11}$ ***b)*** $x_0 = u_{20}, p = u_{21}$ ***c)*** $x_0 = u_{50}, p = u_{51}$.

3.2 Algorithme de Brent

L'algorithme de Floyd permet de trouver une valeur x_i dans le cycle et ensuite la longueur du cycle et la longueur de la pré-période en considérant la suite d'indices $(i, 2i)$ et en testant l'égalité $x_i = x_{2i}$. L'algorithme de Brent utilise la suite (i, j) et teste l'égalité $x_i = x_j$. La suite (i, j) est construire en partant de $(0, 1)$ et telle que

$$\begin{array}{lcll} (i,j) & \mapsto & (i,j+1) & \text{si} \quad j \leq 2i \\ (i,j) & \mapsto & (j,j+1) & \text{si} \quad j = 2i+1 \end{array}$$

Question 6 *Donner la valeur de i et j trouvés par cet algorithme pour la suite $(x_k)_{k\geq 0}$ des itérés de f_p à partir de x_0 :*
a) $x_0 = u_{10}, p = u_{11}$ ***b)*** $x_0 = u_{20}, p = u_{21}$ ***c)*** $x_0 = u_{50}, p = u_{51}$.

Question à développer pendant l'oral : Quel avantage voyez-vous à utiliser l'algorithme de Brent par rapport à celui de Floyd ?

3.3 Application à la factorisation

La méthode ρ de Pollard permet de factoriser un entier N en utilisant un algorithme de recherche de cycle. Considérons la suite (x_i, x_j) définie par l'algorithme de Brent appliqué à la fonction suivante $f(x) = (x^2 + c) \bmod N$.
On suppose que la suite $(x_i - x_j)$ vérifie la propriété

$$\exists (i, j) \text{ et } q > 1 \text{ tels que } q \text{ divise à la fois } (x_i - x_j) \text{ et } N.$$

Question 7 *En utilisant l'algorithme de Brent avec $c = 11$ et en partant de $x_0 = 2$, donner les valeurs de i, j et du facteur de N différent de 1 et N pour*
a) $N = u_{10}$ ***b)*** $N = u_{20}$ ***c)*** $N = u_{50}$.

4 Recherche de cycle dans un ensemble ordonné

Nous allons dans cette section utiliser le fait que E est muni d'un ordre total.

Considérons l'algorithme suivant qui calcule les valeurs de la suite et stocke certains (x_i, i) dans un ensemble F. F est initialement vide. À l'étape j, si x_j est déjà présent dans F, l'algorithme s'arrête. Sinon, retirer de F toutes les entrées (x_i, i) telles que $x_i > x_j$ puis ajouter (x_j, j) à F et continuer.

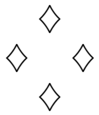
Question à développer pendant l'oral : Quelle est la propriété de la valeur sur laquelle l'algorithme se termine ? En déduire comment calculer la longueur du cycle.

Question 8 *Donner les valeurs de x_i et i au moment où l'algorithme se termine ainsi que la taille maximale de l'ensemble F pour la suite $(x_k)_{k\geq 0}$ des itérés de f_p à partir de x_0 :*
a) $x_0 = u_{10}, p = u_{11}$ ***b)*** $x_0 = u_{20}, p = u_{21}$ ***c)*** $x_0 = u_{50}, p = u_{51}$.

Une variante de l'algorithme précédent consiste à diviser l'ensemble E en K classes disjointes munies chacune de son ensemble de (x_i, i). On considère ici les classes d'équivalence modulo $K = 1000$. À l'étape i, on détermine à quelle classe x_i appartient et on ajoute (x_i, i) à l'ensemble correspondant.

Question 9 *Donner les valeurs de x_i et i au moment où l'algorithme se termine pour la suite $(x_k)_{k\geq 0}$ des itérés de f_p à partir de x_0 :*
a) $x_0 = u_{10}, p = u_{11}$ ***b)*** $x_0 = u_{20}, p = u_{21}$ ***c)*** $x_0 = u_{50}, p = u_{51}$.

Question à développer pendant l'oral : Quel est l'intérêt de cette dernière technique par rapport à la précédente ?



Fiche réponse type: Le Lièvre et la Tortue

$\widetilde{u_0}$: 33

Question 1

a) (21181, 204597202)

b) (2464, 106192576)

c) (16080, 241656996)

Question 2

a) (787, 522)

b) (870, 969)

c) (1195, 894)

Question 3

a) (14587, 36854, 50009)

b) (6189, 49088, 53820)

c) (42258, 1691, 43087)

Question 4

a) (36854, 190075797)

b) (49088, 226981518)

c) (42275, 83919148)

Question 5

a) (161070466, 72243002)

b) (186015437, 81988527)

c) (15074231, 187824396)

Question 6

a) (65535, 102389)

b) (65535, 114623)

c) (65535, 67226)

Question 7

a) (59, 15, 24)

b) (28, 1, 3)

c) (12, 1, 3)

Question 8

a) (9000, 82054, 19)

b) (8823, 67529, 25)

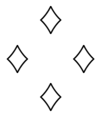
c) (7925, 45531, 30)

Question 9

a) (7292928, 51441)

b) (3000286, 55339)

c) (112026751, 43949)



Fiche réponse: Le Lièvre et la Tortue

Nom, prénom, u_0: .....

Question 1

a)

b)

c)

Question 2

a)

b)

c)

Question 3

a)

b)

c)

Question 4

a)

b)

c)

Question 5

a)

b)

c)

Question 6

a)

b)

c)

Question 7

a)

b)

c)

Question 8

a)

b)

c)

Question 9

a)

b)

c)