Chaîne d'additions

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

Durée de l'épreuve: 3 heures 30 minutes

Juin 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.

On s'intéresse dans ce sujet au problème du calcul de x^n, étant donnés x et n (n étant un entier positif). Pour calculer x^n rapidement, il est utile de décomposer n : si $n = pq + r$ par exemple, on peut utiliser le fait que $x^n = x^{pq+r} = (x^p)^q \cdot x^r$.

Une chaîne d'additions pour un entier n est une suite d'entiers

$$1 = a_0, a_1, a_2, \ldots, a_\ell = n$$

satisfaisant la propriété suivante

$$a_i = a_j + a_k, \text{ pour } k \leq j < i, \text{ pour } i = 1, 2, \ldots, \ell.$$

La chaîne d'additions la plus courte possible minimise le nombre de multiplications et correspond à un algorithme d'exponentiation efficace. Une chaîne d'additions de 23 peut s'écrire :

$$1 \to 2 \to 3 \to 4 \to 7 \to 8 \to 16 \to 23 \tag{1}$$

ou

$$1 \to 2 \to 3 \to 5 \to 10 \to 20 \to 23.$$

La *longueur* de la chaîne $L(n) = (a_i)_{0 \leq i \leq \ell}$ est l'entier ℓ et son *haché* est l'entier défini par

$$H(L(n)) = \left(\sum_{i=1}^{\ell} a_i \right) \bmod 9973.$$

On fera attention à effectuer la réduction modulo 9973 aussi souvent que possible dans le calcul de cette somme !

1 Génération des nombres

On considère la suite d'entiers $(u_k)_{k \geq 0}$ définie pour $k \geq 0$ par :

$$u_k = \begin{cases} \text{votre } u_0 \quad (\textit{À reporter sur votre fiche réponse}) & \text{si } k = 0 \\ 15091 \times u_{k-1} \mod 64007 & k > 0. \end{cases}$$

Question 1 *Donner la longueur et le haché de la chaîne d'additions de la forme* $1 \to 2 \to 3 \to \ldots \to n$ *pour les entiers* n *suivants :*
a) u_{10} **b)** u_{20} **c)** u_{50}.

Dans certaines questions, il pourra être utile de décomposer des entiers n sous forme binaire $n = \sum_{i=0}^{j} n_i \cdot 2^i$ avec $n_i \in \{0, 1\}$ un chiffre binaire (bit) et $n_j \neq 0$. L'écriture de n en base 2 s'écrira $n = n_j \ldots n_2 n_0$.

Question 2 *Donner le nombre total de bits à 1 dans les écritures binaires des entiers compris dans les intervalles suivants :*
a) $[u_{10}; u_{10} + 10]$ **b)** $[u_{20}; u_{20} + 20]$ **c)** $[u_{50}; u_{50} + 50]$.

2 Méthode binaire

Question à développer pendant l'oral : Quelle est la chaîne d'additions minimale pour $n = 2^u$?
Plus généralement, on peut construire une chaîne d'additions efficace en utilisant la décomposition de $n = \sum_{i=0}^{j} n_i 2^i$ en base 2 avec $n_i \in \{0, 1\}$ et $j = \lfloor \log_2(n) \rfloor$. La chaîne comprend d'une part les valeurs 2^i nécessaires et d'autre part les sommes partielles $\sum_{i=0}^{k} n_i 2^i$ pour $k = 0, \ldots, j$. Par exemple, la chaîne (1) donnée plus haut correspond à la chaîne d'additions de 23 avec la méthode binaire.

Question 3 *Donner la longueur et le haché de la chaîne d'additions obtenue avec la méthode binaire pour les valeurs de n suivantes :*
a) u_{10} **b)** u_{20} **c)** u_{50}.

3 Méthode des facteurs

On s'intéresse ici à une méthode qui exploite la factorisation de n de façon récursive.
Si $n = pq$ avec p le plus petit facteur premier de n, on calcule la chaîne d'additions de p, suivie de la chaîne de q multipliée par p. Si n est premier, on utilise la chaîne de $n - 1$ pour produire celle de n. Par exemple, la chaîne de $15 = 3 \times 5$ sera :

$$1 \to 2 \to 3 \to 6 \to 12 \to 15.$$

Question 4 *Quelle est la longueur de la chaîne d'additions otbenue par la méthode des facteurs pour les entiers suivants ?*
a) u_{10} **b)** u_{20} **c)** u_{50}.

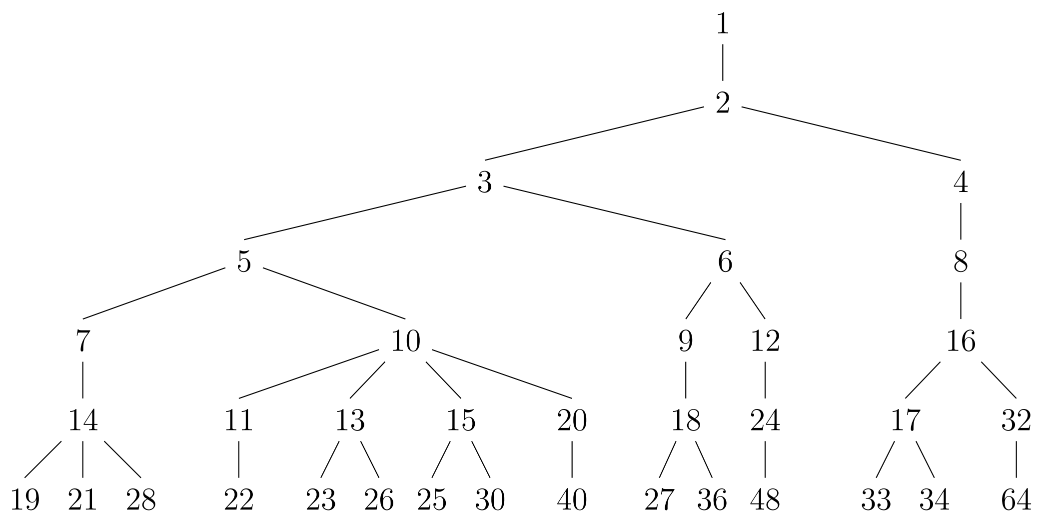
Question à développer pendant l'oral : Quelle est la complexité en temps de votre algorithme ?

4 Méthode de l'arbre des puissances

Une autre méthode consiste à utiliser l'arbre des puissances représenté ci-dessous. Le chemin menant de la racine de l'arbre au nœud n indique une chaîne d'additions pour n. Le $(k + 1)$-ème niveau de l'arbre est défini à partir des k premiers niveaux de la façon suivante : prendre chaque nœud n du k-ème niveau, de gauche à droite, et le relier avec les nœuds

$$n + 1, n + a_1, n + a_2, \ldots, n + a_{k-1} = 2n$$

dans cet ordre, où $1, a_1, a_2, \ldots, a_{k-1}$ est le chemin de la racine de l'arbre à n. On n'ajoutera pas un nœud si celui-ci est déjà présent dans l'arbre.



Question 5 *Donner la longueur et le haché de la chaîne d'additions obtenue à partir de l'arbre des puissances pour les valeurs n suivantes :*
a) $\lfloor u_{10}/64 \rfloor$ **b)** $\lfloor u_{20}/32 \rfloor$ **c)** $\lfloor u_{50}/32 \rfloor$.

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

5 Méthode binaire améliorée

On va s'intéresser ici à une variante de la méthode binaire vue plus haut. Au lieu de lire l'entier n en base 2, on va le lire en base 2^k avec k un entier petit : $n = 2^{jk}c_j + \ldots + 2^{2k}c_2 + 2^k c_1 + c_0$ avec $0 \leq c_i < 2^k$ pour $0 \leq i \leq j$, $c_j \neq 0$ et $jk \leq \log_2(n) < (j+1)k$. On se placera dans le cas $k = 3$.

On considère d'abord la méthode qui calcule en premier de manière naïve les valeurs c_i nécessaires pour $0 \leq i \leq j$ (comme à la question 1) et qui ensuite parcourt l'écriture de n en base 2^k de c_j vers c_0, en utilisant le fait que $n = (((c_j 2^k + c_{j-1})2^k) + \cdots + c_1)2^k + c_0)$. On parle de *fenêtres* de k bits :

$$161 = 2 \cdot 2^{2 \cdot 3} + 4 \cdot 2^3 + 1 = \underbrace{\texttt{010}}_{2}\underbrace{\texttt{100}}_{4}\underbrace{\texttt{001}}_{1}.$$

La chaîne d'additions pour 161 est alors

$$1 \to 2 \to 3 \to 4 \to 8 \to 16 \to 20 \to 40 \to 80 \to 160 \to 161.$$

Question 6 *Donner la longueur et le haché de la chaîne d'additions obtenue par cette méthode pour les valeurs de :*
a) $2^{12} \cdot u_{10} + u_{11}$ **b)** $2^{12} \cdot u_{20} + u_{21}$ **c)** $2^{12} \cdot u_{50} + u_{51}$.

Question à développer pendant l'oral : Quelle est la complexité de votre algorithme en fonction de k et j ? Pour quelle valeur de k la longueur de la chaîne est-elle minimale ?

On considère maintenant une autre méthode binaire qui repose toujours sur la décomposition $n = 2^{jk}c_j + \ldots + 2^{2k}c_2 + 2^k c_1 + c_0$ avec $0 \leq c_j < 2^k$. On note $d(z)$ la somme des

2^{ik} pour tout i tel que $c_i = z$. On commence la chaîne par $1, 2, 4, 8, \ldots, 2^{jk}$. On calcule ensuite les $d(z)$ pour $z = 1, \ldots, 2^k - 1$ comme des sommes de puissances de 2^k qu'on accumule dans l'ordre croissant.

Question à développer pendant l'oral : Montrer qu'on peut calculer efficacement la somme $n = \sum_{z=1}^{2^k-1} zd(z)$ en calculant en même temps les sommes partielles des $d(z)$.

La chaîne d'additions obtenue par cette méthode pour $n = 161$ est alors :

$$1 \to 2 \to 4 \to 8 \to 16 \to 32 \to 64 \to 72 \to 73 \to 88 \to 161.$$

Question 7 *Donner la longueur et le haché de la chaîne d'additions obtenue par cette méthode pour les valeurs de :*

a) $2^{12} \cdot u_{10} + u_{11}$ **b)** $2^{12} \cdot u_{20} + u_{21}$ **c)** $2^{12} \cdot u_{50} + u_{51}$.

6 Chaîne d'additions-soustractions

On s'intéresse au problème de trouver une chaîne d'additions vectorielles, c'est-à-dire trouver une chaîne d'additions minimale pour (n_1, n_2) à partir des vecteurs unités $(1, 0)$ et $(0, 1)$.

Question à développer pendant l'oral : Montrer comment calculer avec l'algorithme de la question 3 une chaîne d'additions pour le vecteur (n_1, n_2) ?

Dans les cas où le calcul de l'inverse est efficace, il peut être utile de décomposer l'entier n sur l'alphabet $\{-1, 0, 1\}$ et représenter n par deux entiers positifs (n_+, n_-) tels que $n = n_+ - n_-$. On remarque que l'on peut améliorer la chaîne obtenue à la question 3 dans le cas $n = 15$:

$$1 \to 2 \to 3 \to 4 \to 7 \to 8 \to 15 \text{ en}$$

$$(1, 0), (0, 1) \to (2, 0) \to (4, 0) \to (8, 0) \to (16, 0) \to (16, 1) = 15.$$

Question à développer pendant l'oral : Montrer que quand l'écriture binaire de n contient un paquet d'au moins deux `1` consécutifs, on peut le remplacer par un bit `1` dans n_+ et un bit à `1` dans n_-.

Question 8 *Donner les valeurs de (n_+, n_-) pour les valeurs de n suivantes en appliquant la méthode de la question orale précédente.*

a) $2^{12} \cdot u_{10} + u_{11}$ **b)** $2^{12} \cdot u_{20} + u_{21}$ **c)** $2^{12} \cdot u_{50} + u_{51}$.

Question à développer pendant l'oral : Montrer que quand l'écriture binaire de n contient un paquet d'au moins deux `1` consécutifs, suivi d'un seul `0` et suivi d'un autre paquet d'au moins deux `1` consécutifs, on peut diminuer encore le nombre de bits à `1` dans n_+ et n_-.

Question 9 *Donner les valeurs de (n_+, n_-) pour les valeurs de n suivantes en utilisant la question orale précédente :*

a) $2^{12} \cdot u_{10} + u_{11}$ **b)** $2^{12} \cdot u_{20} + u_{21}$ **c)** $2^{12} \cdot u_{50} + u_{51}$.

$\diamond$

$\diamond \quad \diamond$

$\diamond$

Fiche réponse type: Chaîne d'additions

$\widetilde{u_0}$: 1

Question 1

a) 11034, 5964

b) 29910, 27

c) 4084, 8226

Question 2

a) 77

b) 190

c) 255

Question 3

a) 20, 1460

b) 23, 3329

c) 20, 2198

Question 4

a) 20, 5668

b) 20, 9793

c) 17, 6398

Question 5

a) 9, 381

b) 13, 2359

c) 10, 410

Question 6

a) 35, 6587

b) 37, 3946

c) 34, 4259

Question 7

a) 36, 559

b) 37, 7708

c) 34, 6752

Question 8

a) n+=46303234,
n-=1056896

b) n+=139597121,
n-=17072128

c)

n+=16814146,
n-=73992

Question 9

a)

n+=46303234,
n-=1056896

b)

n+=139466049,
n-=16941056

c)

n=+16777282,
n-=37128

Fiche réponse: Chaîne d'additions

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)

◇ ◇ ◇ ◇