Librairie de calcul arithmétique en précision arbitraire

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

Durée de l'épreuve: 3 heures 30 minutes

Juillet 2011

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.

1 Introduction

1.1 Notations et recommandations

Le but de cette épreuve est de réaliser une bibliothèque de calcul arithmétique en précision arbitraire. Cela signifie que vous allez devoir programmer différentes opérations de base du calcul sur les entiers (addition, soustraction, multiplication) pour des entiers de longueur arbitraire.
Rappelons qu'en général les processeurs utilisés dans les ordinateurs actuels sont capables d'effectuer ces mêmes calculs sur des entiers dont la longueur est 32 bits (voire 64 bits sur les modèles les plus récents). Cependant dès que l'on souhaite pouvoir faire des calculs sur des entiers de longueur arbitraire, on est obligé de recourir à des librairies de calcul spécialisées. La manipulation de ces grands entiers est très utilisée pour certaines applications comme la cryptographie (par exemple pour la protection de la confidentialité d'un message, ou l'authentification de l'émetteur d'un message).
Soit $b \geq 2$ un entier. On dira qu'un entier $n \geq 0$ s'écrit $x_l x_{l-1} \ldots x_0$ dans la base b, ce que l'on notera $n = x_l x_{l-1} \ldots x_{0|b}$ si et seulement si :

$$\begin{cases} \forall\, 0 \leq i \leq l \quad 0 \leq x_i \leq b-1 \\ \qquad\qquad n = \displaystyle\sum_{i=0}^{l} x_i b^i \end{cases}$$

On peut montrer que cette décomposition est unique, ce qui assure l'unicité de l'écriture d'un entier dans une base b donnée.

Important ! Afin d'obtenir les réponses correctes aux questions du sujet, il est obligatoire d'utiliser comme base $b = 10$.

1.2 Générateur de grands entiers

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

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

Question 1 *Que valent :*
a) u_{30} ***b)*** u_{300} ***c)*** u_{3000}.

Considérons la fonction v définie de $\mathbb{N} \times \mathbb{N}$ vers $\mathbb{N}$ par :

$$v(k,l) = \sum_{i=1}^{l} (u_{kl+i} \mod 10) \times 10^{i-1}.$$

Définition 1 *On appellera signature de l'entier $n \geq 0$, le n-uplet (n_3, n_5, n_7) défini par :*

n_i = le nombre de fois où le chiffre i apparaît dans l'écriture décimale de n.

On la notera $sig(n)$.

Question 2 *Que valent :*
a) $v(1,5)$ ***b)*** $sig(v(2,50))$ ***c)*** $sig(v(10,500))$.

Dépendances entre questions La section 3 dépend de la section 2. La section 4 est indépendante.

2 Opérations de base

2.1 Comparaison

Vous développerez un algorithme permettant la comparaison de deux entiers en précision arbitraire.
Soit $(S_{n,l})_{0\leq i<n}$ la suite de n grands entiers définie par :

$$(S_{n,l})_i = v(i,l).$$

Question 3 *Quelle est la signature du plus grand entier contenu dans les listes suivantes :*
a) $(S_{10,10})$ ***b)*** $(S_{100,100})$ ***c)*** $(S_{200,200})$.

2.2 Addition

Développez un algorithme d'addition pour les grands entiers.

Question 4 *Que valent :*
a) $sig(v(1,50)+v(2,50))$ ***b)*** $sig(v(1,100)+v(2,100))$ ***c)*** $sig(v(1,500)+v(2,500))$.

Question à développer pendant l'oral : Détaillez l'algorithme que vous avez développé. Quelle est la complexité en temps de cet algorithme (en fonction de la taille des entiers à ajouter) ? Pensez-vous qu'il soit possible d'améliorer cette complexité ? Justifiez.

Définition 2 *Soient $x = \sum_{i=0}^{l} x_i 10^i$ et $y = \sum_{i=0}^{l} y_i 10^i$ deux entiers en précision arbitraire. On définit l'opération $\oplus$, de la manière suivante :*

$$(x \oplus y) = \sum_{i=0}^{l} (x_i + y_i) \mod 10.$$

Lorsque x et y n'ont pas le même nombre de chiffres dans leurs représentations en base 10, on étend le plus petit des deux par des zéros en tête pour atteindre la longueur souhaitée.

Lorsque l'on compare le résultat de $x+y$ avec celui de $x \oplus y$, les deux nombres obtenus diffèrent en un certain nombre de positions (dans leurs représentations en base 10). Soit $d(x,y) = \{i \mid (x+y)_i \neq (x \oplus y)_i\}$ l'ensemble des positions où ces deux nombres diffèrent. On notera $\Delta(x,y) = \max\{l \mid \exists i\, \forall j \quad 0 \leq j < l \Rightarrow i+j \in d(x,y)\}$, la longueur de la plus longue séquence d'entiers consécutifs dans $d(x,y)$.

Question 5 *Que valent :*
a) $\Delta(v(1,10), v(2,10))$ ***b)*** $\Delta(v(1,50), v(2,50))$ ***c)*** $\Delta(v(1,500), v(2,500))$.

Question à développer pendant l'oral : Si l'on dispose d'un nombre suffisant d'unités logiques élémentaires capables d'additionner deux nombres compris dans $[0,9]$, quelle information contient $d(x,y)$?

2.3 Soustraction

Vous devez développer un algorithme de soustraction pour les grands entiers. Cet algorithme prendra en paramètre deux entiers a et b, et calculera $\mid a - b \mid$.

Question 6 *Que valent :*
a) $sig(\mid v(1,10) - v(2,10) \mid)$ ***b)*** $sig(\mid v(1,50) - v(2,50) \mid)$ ***c)*** $sig(\mid v(1,500) - v(2,500) \mid)$.

Question à développer pendant l'oral : Détaillez l'algorithme que vous avez développé.

3 Multiplication d'entiers

Question à développer pendant l'oral : Détaillez un algorithme de multiplication de grands entiers. Donnez sa complexité en temps et en espace.

Recommendations L'algorithme à développer dans cette section nécessite de travailler sur des entiers signés. Vous devrez donc prendre en compte le signe des entiers qui apparaîtront au cours du calcul.

Algorithme de Karatsuba (1962) Le mathématicien Carl Friedrich Gauss (1777-1855) a découvert en 1805 le fait suivant à propos de la multiplication des nombres complexes. Soient $x = a + ib$ et $y = c + di$ deux nombres complexes. Le produit de x par y :

$$x \times y = (a + ib)(c + id) = ac - bd + i(bc + ad)$$

semble faire intervenir quatre multiplications. À savoir ac, bd, bc et ad. Cependant Gauss nota qu'il était possible d'obtenir le même résultat en ne faisant intervenir que trois multiplications. En introduisant $\alpha = ac$, $\beta = bd$ et $\gamma = (a + b)(c + d)$, on a en effet $x \times y = \alpha - \beta + i(\gamma - \alpha - \beta)$. En 1960 Karatsuba a redécouvert ce fait et imaginé un algorithme de multiplication basé sur cette remarque.
Plus précisément soient x et y deux grands entiers de même taille l, telle que l soit une puissance de deux :

$$\begin{cases} x = \sum_{i=0}^{2^n - 1} x_i 10^i \\ y = \sum_{i=0}^{2^n - 1} y_i 10^i \end{cases}$$

On peut décomposer x et y en deux nombres de taille égale :

$$\begin{cases} x = x_1 10^{2^{n-1}} + x_0 \\ y = y_1 10^{2^{n-1}} + y_0 \end{cases}$$

On constate que :

$$x \times y = x_1 y_1 10^{2^n} + (x_1 y_0 + y_1 x_0) 10^{2^{n-1}} + x_0 y_0.$$

Ce qui nécessite quatre multiplications. Cependant, en utilisant la même astuce de calcul que celle découverte par Gauss, et en introduisant les entiers suivants :

$$\begin{cases} \alpha = x_1 y_1 \\ \beta = x_0 y_0 \\ \gamma = (x_1 - x_0)(y_1 - y_0) \end{cases}$$

on obtient :

$$x \times y = \alpha 10^{2^n} + (\alpha + \beta - \gamma) 10^{2^{n-1}} + \beta$$

En déduire un algorithme récursif dont le cas de base est la multiplication de deux entiers dans $[0, 9]$ et qui calcule le produit de deux grands entiers (de même taille, une puissance de deux). Pour chacun des résultats demandés, vous donnerez de plus le nombre de multiplications (d'entiers compris dans $[0, 9]$), dont le résultat est non nul, qui ont été nécessaires à l'exécution de votre algorithme.

Question 7 *Donnez la signature des produits suivants (indiquez aussi le nombre de multiplications de deux entiers dans $[0, 9]$ produisant un résultat non nul) :*
a) $sig(v(1, 128) \times v(2, 128))$ ***b)*** $sig(v(1, 256) \times v(1, 256))$ ***c)*** $sig(v(1, 512) \times v(2, 512))$.

Question à développer pendant l'oral : Quelle est la complexité de votre algorithme ? Justifiez votre réponse. Une autre manière de calculer les coefficients α, β et γ est la suivante :

$$\gamma' = (x_1 + x_0)(y_1 + y_0)$$

et on obtient :

$$x \times y = \alpha 10^{2^n} + (\gamma' - \alpha - \beta) 10^{2^{n-1}} + \beta$$

Justifiez pourquoi on n'utilise pas cette méthode en pratique.

4 Ordre d'exécution d'une série de multiplications

Dans cette section, on imagine avoir un algorithme pour la multiplication de deux entiers de tailles respectives l_1 et l_2 dont le coût est égale à $C(l_1, l_2) = (\max(l_1, l_2))^{\frac{3}{2}}$. On considère un ensemble de n grands entiers de longueurs $l_1, \ldots, l_n$ devant être multipliés entre eux. Comme la multiplication est commutative et associative, déterminer le meilleur ordre d'exécution dans lequel doivent être effectuées les multiplications afin de minimiser le coût global nécessite (dans le pire cas) de regarder chacune des permutations possibles pour les nombres à multiplier, et pour chacune de ces permutations de décider d'un parenthésage. Ceci est évidemment prohibitif. On va comparer le coût de plusieurs stratégies.
Soit $(L_n)_{0 \leq k < n}$ la suite de n entiers définie par :

$$(L_n)_k = (u_k \mod 20) + 1.$$

De gauche à droite On décide tout d'abord d'effectuer les multiplications dans l'ordre dans lequel apparaissent les grands entiers.

Question 8 *Que vaut le coût de la multiplication d'une suite d'entiers dont les longueurs (de gauche à droite) sont spécifiées par les suites d'entiers suivantes :*
a) L_5 ***b)*** L_{50} ***c)*** L_{500}.

Par longueurs initiales triées On décide de trier initialement les longueurs des entiers par ordre croissant. Les entiers sont placés dans cet ordre et multipliés de gauche à droite.

Question 9 *Que vaut le coût de la multiplication d'une suite d'entiers dont les longueurs (de gauche à droite) sont spécifiées par :*
a) L_5 ***b)*** L_{50} ***c)*** L_{500}.

À vous de jouer ... Proposez une stratégie qui améliore les résultats précédents. La fiche type (calculée pour $\widetilde{u_0}$) contient les résultats obtenus à l'aide d'une stratégie dont vous essayerez d'égaler le coût (voire de l'améliorer).

Question 10 *Quel est le coût de votre stratégie pour la multiplication d'une suite d'entiers dont les longueurs (de gauche à droite) sont spécifiées par :*
a) L_5 ***b)*** L_{50} ***c)*** L_{500}.

Fiche réponse type: Librairie de calcul arithmétique en précision arbitraire

$\widetilde{u_0}$: 3

Question 1

a) 15365

b) 33699

c) 51671

Question 2

a) 54494

b) [7,6,7]

c) [55,56,51]

Question 3

a) [1,2,0]

b) [10,15,7]

c) [24,22,22]

Question 4

a) [4,9,10]

b) [8,11,12]

c) [49,56,44]

Question 5

a) 3

b) 5

c) 11

Question 6

a) [1,0,0]

b) [6,7,3]

c) [47,56,54]

Question 7

a) [29,30,16], 1693

b) [39,49,54], 5154

c) [111,103,108], 15470

Question 8

a) 4.623e+02

b) 2.143e+05

c) 7.073e+07

Question 9

a) 3.755e+02

b) 1.176e+05

c) 4.413e+07

Question 10

a) 3.440e+02

b) 1.224e+04

c) 4.584e+05

Fiche réponse: Librairie de calcul arithmétique en précision arbitraire

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)

Question 10

a)

b)

c)