Arithmétique des entiers en précision arbitraire

Samy Jaziri

Sujet de khôlle adapté d'une épreuve pratique d'algorithmique et de programmation du concours commun des écoles normales supérieures : Librairie de calcul arithmétique en précision arbitraire (2011).

Préambule

Tous les algorithmes de ce sujet devront être implémentés en ***OCaml****.*

Pour vous mettre dans les conditions du concours, vous n'avez pas le droit d'accéder aux ressources en ligne. Une documentation hors-ligne est mise à votre disposition sur le bureau ($\sim$ `/Desktop`*).*

A la fin du sujet, vous trouverez deux fiches réponses. Vous indiquerez vos réponses sur la première fiche en utilisant, en entrée de vos programmes, le numéro u_0 inscrit sur cette fiche. Vous remettrez cette fiche à l'examinateur en fin de séance. La seconde fiche est un exemple des réponses attendues pour un $\widetilde{u_0}$ particulier.
En ce qui concerne les questions orales de la khôlle, lorsque la description d'un algorithme est demandée, vous devez présenter son fonctionnement de façon schématique, courte et précise. Vous ne devez pas expliquer votre code ligne par ligne! Quand la complexité d'un algorithme est demandée en temps ou en mémoire en fonction d'un paramètre n, on demande l'ordre de grandeur en fonction du paramètre, donné en notation de Landau ($\mathcal{O}(n), \mathcal{O}(\log(n)), \dots$). Prenez des notes lorsque vous préparez une question orale pour retrouver plus rapidement les grandes lignes de votre explication lorsque l'examinateur passe vous voir.
Il est recommandé 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.
Il vous est demandé d'aborder les questions dans l'ordre et de noter vos difficultés à répondre à une question avant de passer à la suivante. Vous pourrez alors pour les aborder avec l'examinateur.
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

Le but de ce sujet est de réaliser une bibliothèque de calcul arithmétique en précision arbitraire. En général les processeurs utilisés dans les ordinateurs actuels sont capables d'effectuer des opérations arithmétiques sur des entiers de longueur fixée.

Préparer une réponse à donner à l'oral

Quel est l'entier le plus grand qui peut être sauvegardé dans la mémoire d'un ordinateur d'architecture `x86` ? `x64` ?

Dès que l'on souhaite pouvoir faire des calculs sur des entiers de précision 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.

Question 1

Après avoir lu l'intégralité du sujet, définissez un type `entier` pour représenter les entiers de précision arbitraire.

Préparer une réponse à donner à l'oral

Vous devrez motiver le choix des structures de données utilisées.

Différents algorithmes existent pour réaliser les diverses opérations arithmétiques. Ces algorithmes ne sont pas tous équivalent en termes de complexité. Par exemple x à la puissance n, où x est un nombre flottant et n un entier, peut être calculé naïvement en $\mathcal{O}(n)$ multiplications ou en utilisant l'algorithme d'exponentiation rapide qui utilise $\mathcal{O}(\log n)$ multiplications.

Question 2

Implémentez une fonction `puissance : float → int → float` qui prend en paramètre un flottant x et un entier n et utilise l'algorithme d'exponentiation rapide pour calculer x^n

Préparer une réponse à donner à l'oral

Vous devrez donner la preuve de terminaison, la preuve de correction et l'analyse de complexité de cet algorithme.

Nous nous intéresserons ici à la complexité des différentes opérations que nous allons implémenter. Pour la multiplication de deux entiers, il existe en particulier, en plus de la méthode classique, de nombreux algorithmes de multiplication : méthode égyptienne, méthode par jalousies, algorithme de Schrönage-Strassen, algorithme de Toom-Cook, ... Nous implémenterons l'algorithme de Karatsuba qui est le plus efficaces pour des nombres avec quelques centaines de chiffres.

Générateur d'entiers de précision arbitraire

Dans la suite, les fonctions que vous implémenterez devront travailler sur des entiers en précision arbitraire (i.e de type `entier`).

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

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

Question 3

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

Considérons la fonction $v : \mathbb{N} \times \mathbb{N} - > \mathbb{N}$ telle que :

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

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

$$n_i = \textit{le nombre de fois où le chiffre } i \textit{ apparaît dans l'écriture décimale de } n$$

On la notera `sig`(n).

Attention : `sig` est un symbole réservé en Ocaml.

Question 4

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

2 Opérations de base

Comparaison

Vous développerez un algorithme permettant le calcul de la somme de deux entiers en précision arbitraire.
Pour tous entiers n, l, soit $(S_{n,l})_{0\leq i<n}$ la suite de n entiers définie par

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

Question 5

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

Addition

Développez un algorithme d'addition pour deux entiers en précision arbitraire.

Question 6

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

Préparer une réponse à donner à l'oral

Expliquez l'algorithme que vous avez utilisé. Quelle est sa complexité en temps en fonction de la taille des deux entiers à ajouter ? Pensez-vous qu'il soit possible d'améliorer cette complexité ?

Soustraction

Développez un algorithme qui calcule la différence de deux entiers en précision arbitraire. Cet algorithme prendra en paramètre deux entiers a et b, et calculera $|a - b|$.

Question 7

Que valent :
a) `sig`$(v(1,10) - v(2,10))$ **b)** `sig`$(v(1,50) - v(2,50))$ **c)** `sig`$((v(1,500) - v(2,500))$

Préparer une réponse à donner à l'oral

Expliquez l'algorithme que vous avez utilisé.

3 Multiplication par l'algorithme de Karatsuba (1962)

Préparer une réponse à donner à l'oral

Proposez un algorithme (sans l'implémenter) de multiplication d'entiers en arbitraire. Donnez sa complexité en temps et en espace.

Redécouvrant une technique mise en lumière en 1805 par le mathématicien Carl Friedrich Gauss (1777-1855) pour la multiplication de nombres complexes, Anatoli Alekseïevitch Karatsuba (1937-2008) imagine en 1960 un algorithme de multiplication utilisant la méthode diviser pour régner. Soient x et y deux entiers de même longueur 2^n, $n \in \mathbb{N}$:

$$x = \sum_{i=0}^{2^n-1} x_i \, 10^i \quad , \quad y = \sum_{i=0}^{2^n-1} y_i \, 10^i$$

On peut décomposer x et y en deux nombres de tailles égales :

$$x = x_1 \, 10^{2^{n-1}} + x_0 \quad , \quad y = y_1 \, 10^{2^{n-1}} + y_0$$

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. Katsuba propose alors d'introduire les entiers suivants :

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

Et remarque que :

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

Implémentez un algorithme récursif, s'appuyant sur cette observation, qui calcule le produit de deux entiers en précision arbitraire de même longueur, une puissance de 2. Le cas de base est la multiplication de deux entiers dans $[\![0, 9]\!]$ de type `int`.

Question 8

Donnez la signature des produits suivants :
a) `sig`$(v(1, 128) \times v(2, 128))$ **b)** `sig`$(v(1, 256) \times v(2, 256))$ **c)** `sig`$(v(1, 512) \times v(2, 512))$

Préparer une réponse à donner à l'oral

Quelle est la complexité de votre algorithme ? Justifiez votre réponse. Une autre manière de réduire le nombre de multiplications est de poser $\gamma' = (x_1 + x_0)(y_1 + y_0)$ 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 ?

Modifiez maintenant votre algorithme pour qu'il puisse calculer le produit de deux entiers en précision arbitraire et de longueur quelconque.

Question 9

Donnez la signature des produits suivants :
a) `sig`$(v(1, 100) \times v(2, 200))$ **b)** `sig`$(v(1, 50) \times v(2, 100))$ **c)** `sig`$(v(1, 128) \times v(2, 512))$

Enfin utilisez l'algorithme d'exponentiation rapide pour implémenter une fonction `puissance_entiers` : `entier` $\to$ `int` $\to$ `entier` qui calcule la puissance d'un entier en précision arbitraire (l'exposant lui est un entier de type `int`).

Question 10

Donnez la signature des puissances suivantes :
a) `sig`$(v(1, 50)^{144})$ **b)** `sig`$(v(1, 100)^{21})$ **c)** `sig`$(v(1, 150)^{12})$

Fiche réponse : Arithmétique des entiers en precision arbitraire

Nom, prénom : DOUZ Nadine $\widetilde{u_0}$: 12

Question 3:

a) 61460

b) 6782

c) 14663

Question 4:

a) 66529

b) (4, 5, 3)

c) (40, 63, 47)

Question 5:

a) (0, 2, 1)

b) (11, 10, 10)

c) (17, 20, 20)

Question 6:

a) (2, 6, 6)

b) (11, 8, 12)

c) (51, 58, 49)

Question 7:

a) (1, 1, 0)

b) (3, 6, 5)

c) (39, 55, 56)

Question 8:

a) (24, 28, 28)

b) (50, 48, 44)

c) (91, 99, 103)

Question 9:

a) (22, 31, 28)

b) (10, 16, 17)

c) (59, 69, 55)

Question 10:

a) (696, 691, 729)

b) (206, 201, 211)

c) (188, 183, 190)