IN 101 - TD 08
17 novembre 2010

Énoncé

ENSTA ParisTech

Le but du TD est la manipulation de matrices. On souhaite créer ces matrices en mémoire et que les différentes fonctions y accèdent. Les matrices seront stockées sous la forme d'un tableau des lignes de type `int **` et chaque case contiendra une ligne de type `int *`, c'est-à-dire un pointeur sur la première case de la ligne.

Exercice 1 : Structure rationnel

1.a] Définir le type "rationnel", écrire une fonction d'initialisation qui prend en entrée deux entiers a et b et retourne l'objet de type rationnel représentant a/b.

1.b] Écrire une fonction qui affiche un tel objet.

1.c] Programmer l'addition et la multiplication de deux rationnels (sans simplification).

1.d] Programmer le PGCD de façon récursive.

1.e] Simplifier l'écriture d'un rationnel en faisant un appel par adresse.

1.f] Écrire une fonction qui prend en entrée deux entiers a et b et calcule le pgcd d et les coefficients de Bézout, et des entiers u et v tels que $au + bv = d$. Les entiers u et v seront des paramètres en entrée de la fonction et seront modifiés par la fonction. (L'algorithme gère l'invariant suivant :

$$\forall i \geq 0, \quad au_i + bv_i = r_i \tag{1}$$

où $r_0 = a$, $r_1 = b$ et r_i est la suite des restes dans l'algorithme d'Euclide $r_{i-1} = q_i r_i + r_{i+1}$. Le pgcd est le dernier reste non nul. Donc, $u_0 = 1, v_0 = 0$ et $v_0 = 0, v_1 = 1$, d'après la définition de r_0 et r_1, et si on reporte dans (1), on obtient les règles pour les suites $(u_i)_{i\geq 0}$ et $(v_i)_{i\geq 0}$: $u_{i+1} = u_{i-1} - q_i u_i$ et $v_{i+1} = v_{i-1} - q_i v_i$. À la fin, on a bien écrit le dernier reste non nul comme une combinaison de a et b.)

1.g] Montrer comment calculer l'inverse de a mod b dans le cas où a est inversible modulo b.

1.h] Soit a, b des entiers tels que $a \geq b \geq 0$. On définit la suite des restes comme précédemment, et donc $0 \leq r_{i+1} < r_i$ et λ tel que $r_\lambda = \text{pgcd}(a, b)$ est le dernier reste non nul. On remarque que par définition, $\lambda = 0$ si $b = 0$ et $\lambda > 0$ sinon. Montrer que si $b > 0$,

$$\lambda \leq \log(b)/\log(\phi) + 1,$$

où $\phi := (1 + \sqrt{5})/2 \approx 1.62$.

1.i] Montrer que l'algorithme d'Euclide s'exécute en temps $O(\text{len}(a)\text{len}(b))$ où $\text{len}(a)$ est la longueur de a en bits.

Exercice 2 : Gestion des grands nombres pour calculer 100!

On souhaite calculer avec de grands nombres qui dépassent 32 bits. On va stocker des entiers de 200 digits (chiffres décimaux) dans un tableau en base 100. Dans la case `i`, on mettra le $(2i)^{\text{ieme}}$ et $(2i+1)^{\text{ieme}}$ digits. Un tel entier sera de type : `int digit[100];`. On définira une structure de type `entierlong` qui contiendra ce tableau dans un champ et un autre champ qui contiendra la longueur effective de l'entier. Par exemple, l'entier `9876543201` sera de longueur `5` et le tableau contiendra `digit[0]=01`, `digit[1]=32`, `digit[2]=54`, `digit[3]=76`, `digit[4]=98`, et `digit[i]=0` pour $i = 5$ à 99. Ici, la longueur vaut 4.

Pensez qu'en général, une fonction ne retourne pas une structure, mais plutôt un pointeur sur la structure pour éviter de recopier les valeurs au moment du retour.

2.a] Pourquoi le type `int` ou `long long` ne sont pas suffisant ?

2.b] Écrire la structure `entierlong`. Expliquer ce que retourne votre structure quand vous écrivez `return` suivi d'une telle structure (bien expliquer surtout le tableau) ?

2.c] Écrire une fonction qui affiche un tel nombre sans afficher les zéros en tête. (Faites attention, au cas où la case contient deux digits qui s'écrivent comme un seul : par exemple, la case `digit[0]` contient `01`.)

2.d] Écrire une fonction qui prend un entier < 100, qui initialise une structure de type `entierlong` et la retourne.

2.e] Écrire une fonction qui réalise l'addition de deux tels nombres et retourne une structure contenant le résultat. (Pensez à réserver l'espace mémoire pour ce nouvel entier et n'oubliez pas la retenue !)

2.f] Écrire une fonction qui effectue la multiplication d'un tel nombre et d'un entier ≤ 100.

2.g] Écrire une fonction qui calcule factoriel (100), `100!`.

Exercice 3 : RSA (Groupe fort)

Soit $N = pq$ où p et q sont deux grands nombres premiers. On note $\varphi(N) = (p-1)(q-1)$. Soit e un entier tel que $\text{pgcd}(e, \varphi(N)) = 1$ et d son inverse $\text{mod}\varphi(N)$.

3.a] Écrire une fonction qui réalise le crible d'Ératosthène pour générer des nombres premiers.

3.b] Écrire une fonction qui réalise la multiplication de deux entiers longs.

3.c] Écrire une fonction qui calcule le quotient et le reste de la division de deux entiers longs.

3.d] Écrire la fonction d'addition, de multiplication, d'exponentiation modulo N ainsi que la fonction qui calcule d à partir de e et $\varphi(N)$.

3.e] Implémenter RSA en chiffrement, calculer $m^e \bmod N$ et en déchiffrement $c^d \bmod N$.