Exercice 1 :

1.

#include <studio.h>

int factorielle(int n){

int r = 1;

for (int i = 1 ; i <= n ; i++){

r = r \* i;

}

return r;

}

2.

Le variant de la boucle est : n – i. Car n-i décroit jusqu’à 0

Elle se termine car a un moment dans l’itération de la boucle i sera strictement supérieur à n car n et i sont entiers et varient de 1 à chaque itération (c’est une boucle bornée)

Correction :

Variant : y = n-i

i n – i 0

Donc y = n-I 0 pour chaque itération de la boucle. i est strictement croissant.

Donc n – i va être strictement décroissant.

Donc y est un variant de la boucle.

Donc la boucle se termine pour tout entier n.

D’où la fonction fact termine.

R = (i-1)! Ou au début i=1 , i! = 1 = r

Soit une itération de la boucle et soit r0 et i0 les valeurs de r et i au début de l’itération.

r = (i-1)!

r = (i0 – 1)! i0

= i0!

Et l’incrémente donc i = i0 + 1

Donc r = i0 !

Donc r = i0! = (i-1)!

Donc r = (i-1)! Est un invariant de la boucle et à la fin de la boucle : i = n+1 donc r = n !

Exercice 2 :

1.

ap = a2q+r = ar (a2)q ou q et r sont le quotient et le reste dans la division euclidienne de p par 2.

a21 = a (a2)10

= a (a4)5

= a a4 (a8)2

= a a 4 a16

Entrée : a et p entiers

r = 1

aBis = a

pBis = p

Tant que pBis 0 :

Si pBis % 2 == 1 :

r = r aBis

aBis = aBis aBis

pBis = pBis // 2

Renvoyer r

3.

Variant de boucle :

nBis est entier ; à chaque itération de boucle, nBis > 0

On note nBis(i) la valeur de nBis à la ieme itération de la boucle :

nBis(n+1) = nBis(i)/ 2 < nBis(i)

nBis est strictement décroissant, donc nBis est un variant de la boucle.

La boucle termine donc la fonction exponentiation rapide termine.

4. Invariant de boucle

Valeurs : a, n, r ,aBis, nBis

Montrons que : an = r aBisnBis est invariant dela boucle

Début : r = 1, aBis = a et nBis = n

Donc r aBisnBis = an

Soit r0, a0, et n0 les valeurs de aBis et nBis au début d’une itération de la boucle.

Supposons que r aBisnBis = an .

A la fin de l’itération :

r = r0 a0r’ , où r’ est le reste dans la division euclidienne de n0 par 2.

aBis = a02

nBis = q, le quotient dans la division euclidienne de n0 par 2.

R aBisnBis = r0 a0r’ (a02)q = r0 a02q+r’ = r0 a0n0 = an

Donc la propriété r aBisnBis = an

Est un invariant de la boucle

A la fin de la boucle, nBis = 0, donc r aBisnBis = r = an

Donc la fonction exponentiation rapide est correcte.

5. k+1 tous de boucles sont effectués quand j = 2k

6. Le nombre d’itérations de la boucle est majoré à un facteur contenant près par log2(j) et le nombre d’opérations si chaque itération est bornée : la complexité est O(log2(j))