TP info 9
Corrigé

I1 - Factorielle

Algorithme 1 : Calcul de n !

Entrées : entier naturel n
Sorties : entier naturel fact

```
c=0
fact=1
tant que c<n faire
    c=c+1
    fact=fact*c
retourner fact
```

Suites : $(c_i)_{i\in\mathbb{N}} = \begin{cases} c_0 = 0 \\ c_{i+1} = c_i + 1 \end{cases}$

$(f_i)_{i\in\mathbb{N}} = \begin{cases} f_0 = 1 \\ f_{i+1} = f_i \times c_{i+1} \end{cases}$

1/ Montrons que l'algo termine.
Variant de boucle (c_i) (*)

① Dans la boucle $c_i < n$

② $\begin{cases} c_0 = 0 \\ c_{i+1} = c_i + 1 \end{cases} \Rightarrow \forall i,\ c_i \in \mathbb{N}$

③ $c_{i+1} = c_i + 1 \Rightarrow \forall i,\ c_{i+1} > c_i$
$\Leftrightarrow$ (c_i) strictement ↗

② et ③ $\Rightarrow \exists n$ tq $c_n \geq n$
donc on sort de la boucle
donc l'algo termine

2/ Mq l'algo est correct,
$\Leftrightarrow$ fact = n! à la fin de l'algo.
Mq $(\mathcal{P}_i)$: $f_i = i!$ est un invariant de boucle.

① Initialisation :
$f_0 = 1$
or $1 = 0!$
donc $f_0 = 0!$
donc $\mathcal{P}_0$ vraie

② Hérédité :
Mq $(\mathcal{P}_i) \Rightarrow (\mathcal{P}_{i+1})$.
$f_{i+1} = f_i \times c_{i+1}$
or $c_{i+1} = i + 1$
donc $f_{i+1} = f_i \times (i+1)$
or par hyp $f_i = i!$
donc $f_{i+1} = i!(i+1) = (i+1)!$
donc $(\mathcal{P}_i) \Rightarrow (\mathcal{P}_{i+1})$

Donc $(\mathcal{P}_i)$: $f_i = i!$ est invariant de boucle.

③ En particulier, à la dernière itération on a
$c = n \Rightarrow i = n \Rightarrow f_n = fact = n!$ $(\mathcal{P}_n)$
L'algorithme est correct.

(*) Variant de boucle : $u = n - c \Rightarrow (u_i)_{i\in\mathbb{N}} \begin{cases} u_0 = n \\ u_{i+1} = n - c_{i+1} = u_i - 1 \end{cases}$

① $\begin{cases} u_0 = n \in \mathbb{N} \\ u_{i+1} = u_i - 1 \end{cases} \Rightarrow \forall i,\ u_i \in \mathbb{N}$

② Ds la boucle $\forall i,\ c_i < n$ donc $\forall i,\ u_i = n - c_i > 0$

③ $\forall i,\ u_{i+1} = u_i - 1 \Rightarrow u_{i+1} < u_i \Leftrightarrow (u_i)$ ↘

① et ③ $\Rightarrow \exists$ un rang p tq $u_p < 0$
donc on sort de la boucle : l'algo termine

I 3. Division euclidienne

```
def div_euclidienne(a,b):
    """
    a,b : int, dividende et diviseur a>=0 et 0<b<=a
    q,r : int, quotient et reste de la divison euclidienne de a par b
    """
    r=a
    q=0
    while r>=b:
        r=r-b
        q=q+1
    return q,r
```

r_i $\begin{cases} r_0 = a \\ r_{i+1} = r_i - b \end{cases}$

q_i $\begin{cases} q_0 = 0 \\ q_{i+1} = q_i + 1 \end{cases}$

1/

i	q	r	a	b
0	0	224	224	38
1	1	186		
2	2	148		
3	3	110		
4	4	72		
5	5	34		

2/ Terminaison

Variant de boucle :

(1) $\forall i \quad r_0 = a \in \mathbb{N}$ et $r_{i+1} = r_i - b \in \mathbb{N}$

$\Rightarrow \forall i \quad r_i \in \mathbb{N}$: suite entière,

(2) $\forall i \quad r_{i+1} = r_i - b \Rightarrow \forall i, r_{i+1} < r_i$ suite $\searrow$

(3) Dans la boucle $\forall i, r_i \geq b$.

$\Rightarrow$ une itération n tq $r_n < b$ donc l'algorithme termine.

3/ A l'itération n, à la sortie de la boucle :

$\mathcal{P}_n$: $a = bq_n + r_n$, $r_n < b$

Le invariant de boucle :

$\mathcal{P}_i$: $a = bq_i + r_i$ à montrer

(1) Initialisation : $i = 0$

$r_0 = a$

$q_0 = 0$

or $a = b \times 0 + a$

$a = b \times q_0 + r_0$

donc $\mathcal{P}_0$ vraie

(2) Hérédité : Pq $\mathcal{P}_i \Rightarrow \mathcal{P}_{i+1}$

Hyp : $\mathcal{P}_i$: $a = bq_i + r_i$

Calculons $bq_{i+1} + r_{i+1} = b(q_i + 1) + r_i - b$

$= bq_i + \cancel{b} + r_i - \cancel{b}$

$= bq_i + r_i = a$

(3) Conclusion

A la sortie de la boucle : $i = n$ avec

$\begin{cases} r_n < b \\ a = q_n b + r_n \end{cases}$ donc l'algorithme réalise bien la division euclidienne de a par b

I2- Algorithme sur un tableau

Entrées : tableau de nombres réels de taille N
Sorties : maximum m du tableau

```
m=tableau[0]
pour i de 1 à longueur(tableau)-1 faire
    si tableau[i]>m alors
        m=tableau[i]
retourner m
```

1/ L'algorithme renvoie le maximum du tableau.

2/ Terminaison.

Mq l'algorithme termine. : boucle for donc le compteur finit par dépasser longueur(tableau - 1)

3/ Preuve

Mq l'algorithme renvoie le maximum du tableau au moyen d'un invariant de boucle.

Au rang n (sortie de boucle), l'invariant de boucle doit s'écrire :

m est le maximum du tableau soit : $\forall k \leq n$, $m \geq$ tableau[k]. $(\mathcal{P}_n)$

↳ idée d'invariant à l'itération i : $\forall k \leq i$, $m \geq$ tableau[k] $(\mathcal{P}_i)$

① Montrons $(\mathcal{P}_0)$. Pour $i=0$, $m =$ tableau[0] $\Rightarrow$ $m \geq$ tableau[0]
$(\mathcal{P}_0)$ vrai.

② Hérédité : mq $(\mathcal{P}_i) \Rightarrow (\mathcal{P}_{i+1})$

A l'itération i+1 :

- soit $m \geq$ tableau[i+1]
  et d'après $\mathcal{P}_i$: $\forall k \leq i$, $m \geq$ tableau[k]
  $\Rightarrow$ $\forall k \leq i+1$, $m \geq$ tableau[k]
  donc $(\mathcal{P}_i) \Rightarrow (\mathcal{P}_{i+1})$

- soit $m <$ tableau[i+1]
  alors $m \leftarrow$ tableau[i+1] donc $m =$ tableau[i+1]
  et d'après $\mathcal{P}_i$: $\forall k \leq i$, $m \geq$ tableau[k]
  $\Rightarrow$ $\forall k \leq i+1$, $m \geq$ tableau[k]
  donc $(\mathcal{P}_i) \Rightarrow (\mathcal{P}_{i+1})$

Donc $(\mathcal{P}_i) \Rightarrow (\mathcal{P}_{i+1})$

Donc $(\mathcal{P}_i)$: $\forall k \leq i$, $m \geq$ tableau[k] est invariant de boucle.

③ A l'itération n, le tableau a été entièrement parcouru et l'invariant de boucle reste vrai soit.

$\forall k \leq n$, $m \geq$ tableau[k] i.e. m est le maximum du tableau.

I3 - Pgcd

1/ Pgcd de 144 et 33 suivant l'algo d'Euclide.

144	33
132	4
12	

33	12
24	2
9	

12	9
9	1
3	

9	3
0	3

d'où pgcd(144, 33) = 3

2/ (D_i) $\begin{cases} D_0 = a \\ D_{i+1} = d_i \end{cases}$ (d_i) $\begin{cases} d_0 = b \\ d_{i+1} = r_i \end{cases}$ (r_i) $\begin{cases} r_0 = a \% b \\ r_{i+1} = D_i \% d_i \end{cases}$

Def de la div euclienne : $\begin{cases} D_i = q_i d_i + r_i \\ \text{avec } r_i < d_i \end{cases}$

Terminaison.

(r_i) variant de boucle ?

- $r_i \in \mathbb{N}$ par def de la div. euclienne
- $r_i \in \mathbb{N}$ et dans la boucle $r_i \neq 0$ $\iff$ $r_i > 0$
- $\forall i$, $D_i = q_i d_i + r_i$, $r_i < d_i$ ou $d_i = r_{i-1}$

d'où $\forall i$, $r_i \leq r_{i-1} - 1$ $\iff$ (r_i) strictement

(r_i) est un variant de boucle et l'algo termine.

3/ Correction.

Pq $\mathcal{D}(D) \cap \mathcal{D}(d) = \mathcal{D}(a) \cap \mathcal{D}(b)$ est un invariant de boucle

$\mathcal{D}(D)$: ensemble des diviseurs de D

$\mathcal{D}(d)$: ensemble des diviseurs de d

$\mathcal{D}(D) \cap \mathcal{D}(d)$: ensemble des diviseurs communs à D et d

* Initialisation. $i = 0$. $D = D_0 = a$, $d = d_0 = b$

$\mathcal{D}(D) \cap \mathcal{D}(d) = \mathcal{D}(a) \cap \mathcal{D}(b)$ OK

* Hérédité : $\mathcal{P}_i$: $\mathcal{D}(D_i) \cap \mathcal{D}(d_i) = \mathcal{D}(a) \cap \mathcal{D}(b)$

$\mathcal{P}_{i+1} = \mathcal{D}(D_{i+1}) \cap \mathcal{D}(d_{i+1}) = \mathcal{D}(a) \cap \mathcal{D}(b)$

Mq : $\mathcal{D}(D_{i+1}) \cap \mathcal{D}(d_{i+1}) = \mathcal{D}(D_i) \cap \mathcal{D}(d_i)$

par double inclusion..

(a) $D_i = q_i d_i + r_i \Leftrightarrow D_i - q_i d_i = r_i$

$\Leftrightarrow D_i - q_i d_i = d_{i+1}$.

$\Rightarrow \mathcal{D}(D_i) \cap \mathcal{D}(d_i) \subset \mathcal{D}(d_{i+1})$

$\Rightarrow \mathcal{D}(D_i) \cap \mathcal{D}(d_i) \cap \mathcal{D}(D_{i+1}) \subset \mathcal{D}(d_{i+1}) \cap \mathcal{D}(D_{i+1})$

$D_{i+1} = d_i \quad \mathcal{D}(d_i)$

$\Rightarrow \mathcal{D}(D_i) \cap \mathcal{D}(d_i) \subset \mathcal{D}(d_{i+1}) \cap \mathcal{D}(D_{i+1})$

(b) $D_i = q_i \underbrace{d_i}_{D_{i+1}} + \underbrace{r_i}_{d_{i+1}} \Leftrightarrow D_i = q_i D_{i+1} + d_{i+1}$

$\Rightarrow \mathcal{D}(D_{i+1}) \cap \mathcal{D}(d_{i+1}) \subset \mathcal{D}(D_i)$

$\Rightarrow \mathcal{D}(D_{i+1}) \cap \mathcal{D}(d_{i+1}) \cap \mathcal{D}(d_i) \subset \mathcal{D}(D_i) \cap \mathcal{D}(d_i)$

$\mathcal{D}(D_{i+1})$

$\Rightarrow \mathcal{D}(D_{i+1}) \cap \mathcal{D}(d_{i+1}) \subset \mathcal{D}(D_i) \cap \mathcal{D}(d_i)$

D' où :

$\mathcal{D}(D_{i+1}) \cap \mathcal{D}(d_{i+1}) = \mathcal{D}(D_i) \cap \mathcal{D}(d_i)$

$= \mathcal{D}(a) \cap \mathcal{D}(b)$

(3) Sortie de boucle : $i = n$

(*) $D_n = q_n d_n + r_n$. avec $r_n = 0$

(**) $\mathcal{D}(D_n) \cap \mathcal{D}(d_n) = \mathcal{D}(a) \cap \mathcal{D}(b)$

(*) $\Rightarrow$ $pgcd(D_n, d_n) = d_n$

(**) $\Rightarrow$ $pgcd(D_n, d_n) = pgcd(a, b)$

$\Rightarrow$ $pgcd(a, b) = d_n$