

Exercice 8

8.1) Preuve de la terminaison

Soient $(a, b) \in \mathbb{N}^+ \times \mathbb{N}^+$
 Supposons par l'absurde
 que $\text{Multiplie1}(a, b)$ ne se ter-
 mine pas. Notons la suite
 $(M_n)_{n \in \mathbb{N}}$ la suite de valeurs
 que prendra la variable m .
 On a $\forall n \in \mathbb{N}, M_{n+1} = M_n + 1$
 d'après le code.
 Donc $(M_n)_{n \in \mathbb{N}}$ est strictement
 croissante.
 On a aussi que $\forall n \in \mathbb{N}$
 $M_n < a$ (condition de boucle)
 Donc (M_n) est une suite stricto-
 ment croissante majorée.
 Absurde.
 Donc l'algo se termine avec
 a la fin de boucle.

Preuve de la validité

Notons $(P_n)_{n \in [0, \dots, a]}$ les valeurs
 de p et $(M_n)_{n \in [0, \dots, a]}$
 Montrons que $\forall n, P_n = M_n \times b$ pour
 $\forall n \in [0, \dots, a]$

Base: On a $P_0 = 0$ donc H_0 est vraie

Induction: Soit $n \in [1, \dots, a]$. On
 suppose H_{n-1} vraie et on veut mon-
 trer que H_n aussi.

$$\begin{aligned} \text{On a } P_n &= P_{n-1} + b \text{ d'après le code} \\ &= (n-1)b + b \\ &= nb \end{aligned}$$

donc H_n est vraie.

En sortie de boucle, la valeur de
 p est $P_a = a \times b$ par H_a
 donc la valeur de p retournée
 correspond bien au résul-
 tat attendu.

8.2) la boucle tant que de
 Multiplie1(a, b) fait a itérations.
 Pour chaque itération, deux
 opérations additions sont
 réalisées.

- la première est en $O(\log(ab))$ car la
 variable p prend des valeurs
 inférieures ou égales à $a \times b$.

- la deuxième est en $O(\log(a))$ car la
 variable m vaut toujours
 moins que a .

$$\Rightarrow O(a \log(ab))$$

Exercice 9

$$a = 4, b = 11$$

9.1)

k	prod	x	y
0	0	4	11
1	4	8	5
2	4+8=12	16	4
3	12	32	1
4	44	64	0

$$\hookrightarrow \text{prod} = 44$$

9.2)

Soient $(a, b) \in \mathbb{N}^2$.
 On suppose par l'absurde
 que l'algo $M_2(a, b)$ ne se termine
 pas. On aurait alors une
 suite $(y_m)_{m \in \mathbb{N}}$ de valeurs que
 prend la variable y qui véri-
 fierait

$$\begin{aligned} &\rightarrow \forall m \in \mathbb{N}, y_m > 0 \\ &\rightarrow \forall m \in \mathbb{N}, y_{m+1} \leq y_m / 2 < y_m \end{aligned}$$

$\rightarrow \forall m \in \mathbb{N}, y_m \in \mathbb{N}$ car la variable
 y est divisée par 2 lorsqu'elle
 a une valeur paire grâce au
 "si y impair".

On aurait une suite d'entiers
 strictement décroissante minorée.
 Absurde. Donc M_2 termine

~~Gm~~

On note N le nombre de tours de boucle.

Pour $k \in [1 \dots N]$, on note
 y_k la valeur de la variable après le k ième tour de boucle
 x_k la valeur de la variable x après le k ième tour de boucle
 p_k la valeur de ~~la~~ la variable prod après le k ième tour de boucle.

et x_0, y_0, p_0 les valeurs initiales de ces variables

On montre par récurrence que pour tout $k \in [0 \dots N]$

$$p_k + x_k \times y_k = a \times b \quad (H_k)$$

Initialisation : $y_0 = b, x_0 = a, p_0 = 0$

$$\text{donc } p_0 + x_0 \times y_0 = 0 + a \times b = a \times b$$

donc H_0 est vraie.

Soit $k \in [0 \dots N-1]$. On suppose (H_k) vraie

→ Si y_k est pair alors $y_{k+1} = y_k / 2$

~~g~~

$$x_{k+1} = 2x_k$$

$$p_{k+1} = p_k$$

$$\text{donc } p_{k+1} + x_{k+1} \times y_{k+1} = p_k + 2x_k \times \frac{y_k}{2} = p_k + x_k \times y_k = a \times b \text{ par } H_k$$

→ Si y est impair alors

$$y_{k+1} = (y_k - 1) / 2$$

$$x_{k+1} = 2x_k$$

$$p_{k+1} = p_k + x_k$$

$$y_{k+1} = \frac{y_k - 1}{2}$$

$$\text{donc } p_{k+1} + x_{k+1} \times y_{k+1} = p_k + x_k + 2x_k \times \frac{y_k - 1}{2} = p_k + x_k + x_k \times y_k - x_k = p_k + x_k \times y_k = a \times b \text{ par } H_k$$

Donc H_{k+1} est vraie.

Ainsi, on a montré par récurrence que $\forall k \in [0 \dots N], H_k$

En particulier, H_N donne

$$p_N + x_N y_N = a \times b$$

→ Si $b = 0$, y est initialisé à 0 la boucle tant que n'est pas exécutée c-à-d $N = 0$.

Dans ce cas, la valeur retournée est la valeur initiale de prod, c-à-d 0 qui est bien $a \times b$.

→ Sinon la boucle est exécutée et on sort avec la variable y égale à 0 aut. dit $y_N = 0$.

La propriété ~~H_N~~ H_N donne alors $p_N = a \times b$ et l'algo retourne bien $a \times b$.