Exercice 4 :

```
let nombre_chiffres b n =
  let m = ref n in
  let nb = ref 0 in
  while !m > 0 do
    incr nb;
    m := !m / b
  done;
  !nb
;;
```

- Type :

```
val nombre_chiffres : int -> int -> int = <fun>
```

- Invariant de boucle : En notant p la partie entière de $\frac{\ln n}{b}$:

$$\forall n \in \mathbb{N}^*, \exists! p \in \mathbb{N} : b^p \leqslant n < b^{p+1}$$

$p+1$ est le nombre de chiffres en base b de n.
On considère l'assertion suivante :
« $!nb$ est le nombre de tours de boucles effectués et $!m = \left\lfloor \frac{n}{b^{!nb}} \right\rfloor$ »
◇ Avant d'entrer dans la boucle : $!m = n$ et $!nb = 0$ ce sont bien les valeurs attendues.
◇ supposons l'invariant obtenu après $!nb = k$ tours de boucles.
$!nb$ est incrémenté et devient $k+1$.
On dispose du résultat suivant :
Lemme 1 :
$\forall x \in \mathbb{R}, \forall p \in \mathbb{N}^* : \left\lfloor \frac{\lfloor px \rfloor}{p} \right\rfloor = \lfloor x \rfloor$
Preuve:
Rappelons :

$$\forall y \in \mathbb{R} : p = \lfloor y \rfloor \iff p \in \mathbb{Z} \text{ et } p \leqslant y < p+1$$

On en déduit l'encadrement : $-1 < \lfloor px \rfloor - p\lfloor x \rfloor < p$
Sachant que $\lfloor px \rfloor - p\lfloor x \rfloor \in \mathbb{Z}$, on obtient : $0 \leqslant \lfloor px \rfloor - p\lfloor x \rfloor \leqslant p-1$
puis avec $p > 0$: $\lfloor x \rfloor \leqslant \frac{\lfloor px \rfloor}{p} \leqslant \lfloor x \rfloor + 1 - \frac{1}{n}$
ce qui permet de conclure : $\left\lfloor \frac{\lfloor px \rfloor}{p} \right\rfloor = \lfloor x \rfloor$ ■
On a : $!m = \left\lfloor \frac{n}{b^{!nb}} \right\rfloor$. Posons : $x = \frac{n}{b^{!nb+1}}$ et $p = b \in \mathbb{N}^*$.
Avec le lemme précédent :

$$\left\lfloor \frac{\left\lfloor b \frac{n}{b^{!nb+1}} \right\rfloor}{b} \right\rfloor = \left\lfloor \frac{n}{b^{!nb+1}} \right\rfloor$$

Soit encore :

$$\left\lfloor \frac{!m}{b} \right\rfloor = \left\lfloor \frac{n}{b^{!nb+1}} \right\rfloor$$

Comme $!m$ devient $!m \,/\, b = \left\lfloor \frac{!m}{b} \right\rfloor$ On obtient bien le résultat voulu. ■

- Terminaison : On considère le variant « $(!nb)$ est strictement décroissante »
Immédiatement vérifié avec $b \geqslant 2 > 1$.
- Correction : Rappelons : $b^p \leqslant n < b^{p+1}$
En utilisant l'invariant :
◇ Après p tours de boucles : $!nb = p$ et $1 \leqslant \frac{n}{b^p} < b$ et donc $!m = \left\lfloor \frac{!m}{b^{!nb}} \right\rfloor \in [\![1, b-1]\!]$.
◇ Après $p+1$ tours de boucles : $!nb = p+1$ et $0 \leqslant \frac{1}{b} \leqslant \frac{n}{b^{p+1}} < 1$ et donc $!m = \left\lfloor \frac{!m}{b^{!nb}} \right\rfloor = 0$.
$!nb = p+1$ est bien le nombre de chiffres en base b de n.

m := !m / b
!m strict. > entière naturelle.

```
let ecriture_base b n =
  let nb = nombre_chiffres b n in
  let chiffres = Array.make nb 0 in
  let m = ref n in
  for i = 0 to nb - 1 do
    chiffres.(i) <- !m mod b;
    m := !m / b
  done;
  chiffres
;;
```

- Type :

```
val ecriture_base : int -> int -> int array = <fun>
```

- Invariant de boucle : En notant p la partie entière de $\frac{\ln n}{b}$:

$$\boxed{\exists!(x_0,\dots,x_p)\in[\![0,b-1]\!]^{p+1} : n=\sum_{j=0}^{p} x_j b^j \text{ et } x_p\neq 0}$$

$p+1$ est toujours le nombre de chiffres en base b de n.
On sait que $nb = p+1$.
On considère l'assertion suivante :

Après k tours de boucles : chiffres vaut $[|x_0,\dots,x_{k-1},0\dots,0|]$ et $!m = \sum_{j=k}^{p} x_j b^{j-k}$ »

◇ Avant d'entrer dans la boucle :
$k=0$ et $!m = n = \sum_{j=0}^{p} x_j b^{j-0}$. De plus chiffres est constitué de zéros.
◇ Supposons l'invariant obtenu après k tours de boucles, ie lorsque $i = k-1$.
On sait que :

$$!m = \sum_{j=k}^{p} x_j b^{j-k} = x_k + b(\sum_{j=k+1}^{p} x_j b^{j-k-1})$$

i est incrémenté et devient k
Ainsi, comme $0 \leqslant x_k < b$:

$$!m \ \%\ b \ = x_k$$

Donc chiffres devient $[|x_0,\dots,x_{k-1},x_k,0\dots,0|]$.
De plus :

$$!m \ /\ b = \sum_{j=k+1}^{p} x_j b^{j-(k+1)}$$

ce sont bien les valeurs attendues après $k+1$ tours de boucles, ie lorsque $i=k$. ■

- Terminaison :
On a dans ecriture_base une boucle for donc la terminaison est acquise.
- Correction :
En utilisant l'invariant :
Après $k = nb = p+1$ tours de boucles, ie lorsque $i = nb-1 = p$:
chiffres vaut $[|x_0,\dots,x_{i-1},x_i,\dots,x_p|]$, ce qui est l'écriture de n en base b.

```
let lecture_base b chiffres =
  let nb = Array.length chiffres in
  let n = ref 0 in
  for i = nb - 1 downto 0 do
    n := !n * b + chiffres.(i)
  done;
  !n
;;
```

- Type :

```
val lecture_base : int -> int array -> int = <fun>
```

- Invariant de boucle : En notant p la partie entière de $\frac{\ln n}{b}$:
si $(x_0, \ldots, x_p) \in [\![0, b-1]\!]^{p+1}$ sont les $p+1$ chiffres de x en base b alors :

$$x = \sum_{j=0}^{p} x_j b^j \text{ et } x_p \neq 0$$

On sait que nb est la longueur du tableau chiffres.
Posons $p = nb - 1$
On considère l'assertion suivante :

lorsque $i = k$, on a : $!n = \sum_{j=k}^{p} \text{chiffres.}(j) b^{j-k}$ »

◇ Avant d'entrer dans la boucle, on peut considérer que : $i = nb = p + 1$ et :
$!n = \sum_{j=p+1}^{p} \text{chiffres.}(j) b^{j-k} = 0.$
◇ Supposons l'invariant obtenu lorsque $i = k$.
On sait donc que : $!n = \sum_{j=k}^{p} \text{chiffres.}(j) b^{j-k}$
puis i est décrémenté et i vaut désormais $k - 1$.
Avec n := !n * b + chiffress .(i) $!n$ devient :

$$!n = b \times \sum_{j=k}^{p} \text{chiffres.}(j) b^{j-k} + \text{chiffres.}(k-1) = \sum_{j=k-1}^{p} \text{chiffres.}(j) b^{j-k+1} = \sum_{j=k-1}^{p} \text{chiffres.}(j) b^{j-(k-1)}$$

C'est bien la valeur attendue lorsque $i = k - 1$. ■

- Terminaison :
On a dans lecture_base une boucle for donc la terminaison est acquise.
- Correction :
En utilisant l'invariant, lorsque $i = 0$, on obtient : $!n = \sum_{j=0}^{p} \text{chiffres.}(j) b^j$
On a bien obtenu l'entier dont la liste des chiffres en base b est formée par la tableau chiffres.

Remarque 1 : Si on pose $\forall j \in [\![0, p]\!]$: chiffres.$(j) = x_j$ et $P(X) = \sum_{j=0}^{p} x_j X^j$
Les valeurs successives de $!n$ obtenues sont les étapes du calcul de $P(b)$ par la méthode de Hörner que vous avez (allez) rencontrer dans la chapitre Polynômes.
On a $!n$ qui vaut successivement : x_p puis $x_p b + x_{p-1}$ puis $x_p b^2 + x_{p-1} b + x_{p-2}$ puis ...
puis $x_p b^{p-1} + x_{p-1} b^{p-2} + \cdots + x_2 b + x_1$ et enfin $x_p b^p + x_{p-1} b^{p-1} + \cdots + x_2 b^2 + x_1 b + x_0$
La dernière ligne du tableau d'Hörner contient les valeurs successives de $!n$

	x_p	x_{p-1}	x_{p-2}	$\ldots$	x_0
b		$x_p b$	$x_p b^2 + x_{p-1} b$	$\ldots$	$x_p b^p + x_{p-1} b^{p-1} + \cdots + x_2 b^2 + x_1 b$
	x_p	$x_p b + x_{p-1}$	$x_p b^2 + x_{p-1} b + x_{p-2}$	$\ldots$	$x_p b^p + x_{p-1} b^{p-1} + \cdots + x_2 b^2 + x_1 b + x_0$