Numération en base a.

On fixe a un entier naturel supérieur ou égal à 2. On l'appelle **base de numération**. On se donne aussi a symboles appelés **chiffres** : $X_0, ...X_{a-1}$.
Exemples : écriture décimale ($a = 10$, chiffres =0,1,2,3,4,5,6,7,8,9), écriture binaire ($a = 2$, chiffres=0,1), écriture hexadécimale ($a = 16$, chiffres 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F)

Proposition: pour tout entier m non nul, il existe un unique entier naturel p et un $(p+1)$-uplet $(x_0, \cdots x_{p+1})$ de $\{0\} \cup \mathbb{N}_{a-1}$ tels que

$$m = \sum_{k=0}^{p} x_k a^k \quad \text{et } x_p \neq 0 \quad \text{alors } \overline{X_{x_p} \dots X_{x_0}} \text{ est l'écriture de } m \text{ en base } a.$$

Par convention, $\overline{X_0}$ est l'écriture de 0 en base a.
Exemple: $17 = 16 + 1 = 2^4 + 1 = 3^2 + 2 \times 3 + 1$. Ainsi 17 s'écrit 11 en base 16, 10001 en base 2 et 121 en base 3.

Démonstration: • Existence par récurrence forte sur m. L'hypothèse H_n de récurrence est :"pour tout entier m non nul inférieur ou égal à n, il existe un entier naturel p et une $(p+1)$-liste $(x_0, \cdots x_{p+1})$ de $\{0\} \cup \mathbb{N}_{a-1}$ telle que $m = \sum_{k=0}^{p} x_k a^k$ et $x_p \neq 0$.
— Comme $a > 1$, $H(a-1)$ est vraie car pour $0 < m < a$, on prend $p = 0$ et $a_0 = m$.
— Supposons $H(n)$ vraie. Soit m un entier naturel tel que $0 < m < n+1$. Soit $m < n$ auquel cas l'existence de l'écriture provient de la propriété $H(n)$.
Soit $m = n + 1$. Considérons alors q et r le quotient et le reste de la division euclidienne de m par a. Si $q = 0$ alors $m < a$ et $H(a)$ assure l'existence de l'écriture. Sinon $q \leqslant n$ donc $H(n)$ assure l'existence d'un entier p' et d'une $(p'+1)$-liste $(x'_0, \cdots, x'_{p'})$ tels que $q = \sum_{l=0}^{p'} x'_l a^l$. En prenant $p = p' + 1$ et en considérant la $(p+1)$-liste $(r, x'_0, \cdots x'_{p'})$, on a le résultat.
Ainsi la propriété $H(n)$ est récurrente, vraie au rang a donc vraie d'après le principe de récurrence pour tout n supérieur à a.
• Unicité. Soit $m = \sum_{k=0}^{p} x_k a^k$ avec $x_p \neq 0$ et $0 \leqslant x_k \leqslant a-1$ pour tout k inférieur à p. On a alors $a^p \leqslant x_p a^p \leqslant m \leqslant \sum_{k=0}^{p} (a-1)a^k = a^{p+1} - 1$ autrement dit $a^p \leqslant m < a^{p+1}$. Soit $m = \sum_{k=0}^{q} y_k a^k$ une autre décomposition de m. On a $a^p \leqslant m < a^{q+1}$ d'où $p < q + 1$ soit encore $p \leqslant q$. De même, on obtient $q \leqslant p$ donc $p = q$.
Montrons par l'absurde que $\{n \in N \,|n \leqslant p, x_n \neq y_n\}$ est vide. Si ce n'est pas le cas, cet ensemble est non vide et majoré dans $\mathbb{N}$ donc admet un plus petit élément r. Observons que $\sum_{l=0}^{r} x_l a^l$ est le reste de la division euclidienne de m par a^{r+1}. On a donc $\sum_{l=0}^{r} x_l a^l = \sum_{l=0}^{r} y_l a^l$ et par définition de r, on a $x_l = y_l$ pour tout entier l strictement inférieur à r. Ainsi on obtient $x_r a^r = y_r a^r$ donc $x_r = y_r$ ce qui est la contradiction cherchée.

Remarque: Un entier m est divisible par a^q si et seulement si les q chiffres les plus à droite dans son écriture en base a sont X_0.

Opérations en base a

Soient m et n deux entiers. On les décompose en $m = \sum_{k=0}^{p} x_k a^k$ et $n = \sum_{k=0}^{p} y_k a^k$, les x_k et y_k étant des entiers strictement inférieurs à a. Pour cela, on prend la décomposition en base a et on rajoute des zéros si nécessaire.
On a alors $m + n = \sum_{k=0}^{p} (x_k + y_k) a^k$. Ce n'est pas forcément l'écriture en base a de la somme, comme $x_k + y_k \leqslant 2a - 2 = a + (a - 2)$, on fait une retenue d'au plus une unité.
Finalement on a l'algorithme suivant: `données: p,` $(x_k)_{k\leqslant p}, (y_k)_{k\leqslant p}$ *(Quitte à rajouter des zéros)*
`k=0`
`r=0 (`*retenue*`)`
`Répéter`
`(`s_k`, r) := (reste, quotient) de la division euclidienne de` $x_k + y_k + r$ `par` a
`k:= k+1`
`jusqu'à ce que k=p+1`
`Si r=1 l'écriture est` $X_1 X_{s_p} \cdots X_{s_0}$ `sinon l'écriture est` $X_{s_p} \cdots X_{s_0}$

Exponentiation rapide

On veut calculer α^n.
• Il faut n multiplications par un calcul naïf par récurrence dont l'algorithme est :
`données :` α `et` n
`resultat := 1`
`k :=0 (`*nombre d'itérations*`)`
`Tant que` $k \neq n$
`resultat:=resultat` $\times\alpha$
`k:=k +1;`
`fin tant que`

• On remarque $\alpha^{2p} = (\alpha^2)^p$ et $\alpha^{2p+1} = \alpha(\alpha^2)^p$, d'où l'algorithme dit d'exponentiation rapide
`resultat:=1;`
`exposant:=n`
`a:=`α
`Tant que exposant` $\neq 0$
`si 2 divise exposant alors exposant:=exposant/2`
`sinon exposant := (exposant-1)/2 et resultat:=resultat` $\times a$
`a:=a` $\times$ `a`

Dans chaque boucle, on fait au plus 3 opérations coûteuses (multiplication ou division). Après N opérations, l'exposant vaut au plus $n/2^N$. L'exposant 0 est donc atteint en au plus $1 + P$ itérations où P est le plus petit entier tel que $n/2^P \leqslant 1$ i.e. le plus petit entier $N(n)$ supérieur ou égal à $\ln n / \ln 2$. Finalement, on fait au plus environ $3N(n)$ opérations. D'où une complexité de l'ordre de $O(3 \ln n / \ln 2)$.

Exemples : calcul de α^{345} par exponentiation rapide.

étape	initialisation	1	2	3	4	5	6	7	8	9
exposant	345	172	86	43	21	10	5	2	1	0
nombre d'opérations	0	3	2	2	3	3	2	3	2	3

Soit au total 23 opérations au lieu de 345 par la méthode naïve (remarque : $N(345) = 26$).

n	10	100	10^3	10^5	10^{10}	10^{30}	10^{100}
$N(n)$	10	20	30	50	100	299	997