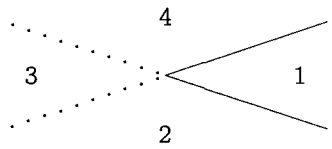
ligne brisée peut être considérée comme deux droites qui se coupent, sauf que les régions situées "après" leur point d'intersection s'unissent pour n'en former qu'une.




Les régions 2, 3 et 4, qui seraient distinctes si on considérait deux droites, constituent une seule région dans le cas d'une ligne brisée. On perd donc deux régions. Deux régions par ligne, c'est tout ce qu'on perdra dans tous les cas si on s'y prend correctement, c'est-à-dire si la brisure se situe "après" les intersections avec toutes les lignes tracées auparavant. Ainsi,

*Voir les détails dans l'exercice 18.*

$$\begin{aligned} Z_n &= L_{2n} - 2n = 2n(2n+1)/2 + 1 - 2n \\ &= 2n^2 - n + 1\,, \qquad \text{pour } n \geqslant 0. \end{aligned} \tag{1.7}$$

En comparant les formules closes (1.6) et (1.7), on trouve que, lorsque $n$ est grand,

$$\begin{aligned} L_n &\sim \tfrac{1}{2}n^2\,, \\ Z_n &\sim 2n^2\,; \end{aligned}$$

donc il y a à peu près quatre fois plus de régions avec des lignes brisées qu'avec des lignes droites. (Nous verrons dans d'autres chapitres comment connaître de façon approchée le comportement d'une fonction entière lorsque $n$ est grand. Le symbole '$\sim$' est défini dans la section 9.1).

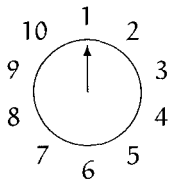
## 1.3 LE PROBLÈME DE JOSÈPHE

*(Ahrens [5, vol. 2] et Herstein et Kaplansky [187] rapportent l'intéressante histoire de ce problème. Josèphe lui-même [197] reste assez vague à ce sujet).*

Notre dernier exemple introductif est une variante d'un problème ancien, à qui on a donné le nom de Flavius Josèphe, célèbre historien du premier siècle. D'après la légende, les fameux talents de mathématiciens de Josèphe lui auraient sauvé la vie. Pendant la guerre entre Rome et les Juifs, il faisait partie d'un groupe de 41 rebelles juifs piégés dans une cave par les Romains. Choisissant de mourir plutôt que d'être capturés, les rebelles décidèrent de former un cercle puis, en suivant sa circonférence, de tuer un homme sur trois comptés parmi les survivants, jusqu'à ce qu'il ne reste plus personne. Josèphe ne voulait pas ce suicide absurde. Il en était de même pour un autre conspirateur, resté anonyme. Alors Josèphe calcula rapidement où son ami et lui devaient se placer dans le cercle vicieux.

*...grâce à quoi nous pouvons lire cette histoire.*

Dans notre variante, on commence avec $n$ personnes numérotées de 1 à $n$ sur un cercle, puis on élimine une personne sur *deux* jusqu'à ce qu'il n'y ait plus qu'un survivant. Voici par exemple la configuration de départ pour $n = 10$ :




On élimine dans l'ordre 2, puis 4, 6, 8, 10, 3, 7, 1, 9 ; le survivant est 5. Le problème posé en général est le suivant : déterminer le numéro $J(n)$ du survivant.

*Voici un cas où poser $n = 0$ n'a aucun sens.*

Nous venons de voir que $J(10) = 5$. On peut conjecturer que $J(n) = n/2$ lorsque $n$ est pair. Le cas $n = 2$ satisfait cette conjecture : $J(2) = 1$. Cependant, l'étude de quelques autres cas nous dissuade vite : la conjecture est fausse pour $n = 4$ et $n = 6$.

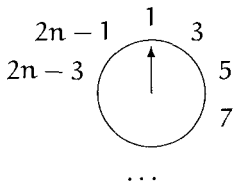
| $n$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $J(n)$ | 1 | 1 | 3 | 1 | 3 | 5 |

*Un mauvaise conjecture n'est pas forcément du temps perdu : cela permet de s'impliquer plus encore dans le problème.*

Remettons-nous au travail pour trouver une meilleure conjecture. Voyons voyons... on dirait que $J(n)$ est toujours impair. Il y a en effet une bonne raison à cela : les nombres pairs sont tous éliminés pendant le premier tour du cercle. De plus, si le nombre $n$ de personnes est lui-même pair, on se retrouve à la fin du premier tour dans une configuration semblable à celle du début, à deux différences près : il reste deux fois moins de participants, et leurs numéros ont changé.

Supposons donc qu'il y a $2n$ personnes au départ. Après le premier tour, on se retrouve avec

*C'est là la ruse : on a $J(2n) = \text{nouveau}(J(n))$, où $\text{nouveau}(k) = 2k - 1$.*




et le prochain candidat choisi sera le 3. C'est exactement comme si on commençait avec $n$ personnes, en ayant toutefois multiplié chaque numéro par 2, puis retranché 1. En d'autres termes,

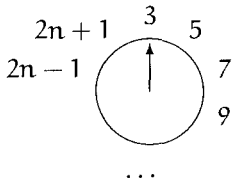
$$J(2n) = 2J(n) - 1, \qquad \text{pour } n \geqslant 1.$$

On peut maintenant calculer rapidement $J(n)$ pour des plus grandes valeurs de $n$. Nous savons par exemple que $J(10) = 5$, donc

$$J(20) \;=\; 2J(10) - 1 \;=\; 2{\cdot}5 - 1 \;=\; 9\,.$$

De même, $J(40) = 17$, et on en déduit aisément que $J(5{\cdot}2^m) = 2^{m+1} + 1$.

Mais que se passe-t-il dans le cas impair ? S'il y a $2n+1$ personnes, la personne numéro 1 est éliminée juste après la personne numéro $2n$, et on se retrouve dans la situation suivante :




On se retrouve encore une fois dans la situation de départ avec $n$ personnes, mais cette fois on a *ajouté* 1 à chaque nombre après l'avoir multiplié par deux. Donc

$$J(2n+1) \;=\; 2J(n) + 1\,, \qquad \text{pour } n \geqslant 1.$$

En ajoutant $J(1) = 1$ à ces équations, on obtient une récurrence qui définit $J$ dans tous les cas :

$$\begin{aligned} J(1) &= 1\,; \\ J(2n) &= 2J(n) - 1\,, \qquad \text{pour } n \geqslant 1; \\ J(2n+1) &= 2J(n) + 1\,, \qquad \text{pour } n \geqslant 1. \end{aligned} \tag{1.8}$$

Cette récurrence est beaucoup plus efficace qu'une relation qui donnerait $J(n)$ en fonction de $J(n-1)$, car elle divise $n$ par deux au moins chaque fois qu'on l'applique. Ainsi, on peut par exemple calculer $J(1000000)$ en n'appliquant que 19 fois (1.8). Cependant nous allons quand même chercher une formule close, parce qu'elle sera plus rapide encore, et plus instructive aussi. N'oublions pas que c'est une question de vie ou de mort !

Avec notre récurrence, on peut écrire très rapidement un tableau des petites valeurs de $J(n)$. Il pourra peut-être nous aider à deviner la réponse.

| $n$ | 1 | 2 3 | 4 5 6 7 | 8 9 10 11 12 13 14 15 | 16 |
|---|---|---|---|---|---|
| $J(n)$ | 1 | 1 3 | 1 3 5 7 | 1 3 5 7 9 11 13 15 | 1 |

Ça y est ! On dirait bien qu'on peut grouper les nombres par puissances de 2, comme indiqué dans le tableau par des traits verticaux. $J(n)$ est toujours égal à 1 au début de chaque groupe, puis il augmente de 2 en 2 dans le même groupe. Ainsi, si l'on pose $n = 2^m + l$, où $2^m$ est la plus

grande puissance de 2 plus petite que $n$ et $l$ représente le reste, il semblerait que la solution de notre récurrence soit

$$J(2^m + l) = 2l + 1, \qquad \text{pour } m \geqslant 0 \text{ et } 0 \leqslant l < 2^m. \tag{1.9}$$

(Notons que si $2^m \leqslant n < 2^{m+1}$, le reste $l = n - 2^m$ satisfait $0 \leqslant l < 2^{m+1} - 2^m = 2^m$).

Il nous faut maintenant prouver (1.9). Nous allons, comme précédemment, utiliser l'induction ; mais cette fois elle portera sur $m$. Si $m = 0$, alors nécessairement $l = 0$ ; ainsi la base de (1.9) est $J(1) = 1$, ce qui est correct. L'étape d'induction comprend deux parties, selon que $l$ est pair ou impair. Si $m > 0$ et $2^m + l = 2n$, alors $l$ est pair et

$$\begin{aligned} J(2^m + l) &= 2J(2^{m-1} + l/2) - 1 \\ &= 2(2l/2 + 1) - 1 = 2l + 1, \end{aligned}$$

de par (1.8) et l'hypothèse d'induction ; c'est exactement ce que nous demandions. Une preuve similaire permet de résoudre le cas impair, lorsque $2^m + l = 2n + 1$. Notons en passant que (1.8) entraîne la relation

$$J(2n + 1) - J(2n) = 2.$$

Quoi qu'il en soit, l'induction est complète et (1.9) établie.

Pour illustrer cette solution, calculons $J(100)$ : comme $100 = 2^6 + 36$, on obtient $J(100) = 2 \cdot 36 + 1 = 73$.

Maintenant que nous avons fait le plus difficile (la solution du problème), voyons quelque chose de plus facile : toute solution d'un problème peut être généralisée pour s'appliquer à une classe plus large de problèmes. Une fois qu'on a appris une technique, il s'avère instructif de l'étudier de près et de voir jusqu'où on peut aller avec. Dans la suite de cette section, nous allons donc examiner la solution (1.9) et explorer quelques généralisations de la récurrence (1.8). Nous allons découvrir grâce à cela la structure qui sous-tend tous les problèmes de ce genre.

Les puissances de 2 ont joué un rôle important dans notre raisonnement. Il est donc naturel de se pencher sur les représentations en base 2 de $n$ et $J(n)$. Supposons que $n$ s'écrit en base 2 comme suit :

$$n = (b_m b_{m-1} \ldots b_1 b_0)_2 .$$

Cela signifie que

$$n = b_m 2^m + b_{m-1} 2^{m-1} + \cdots + b_1 2 + b_0 ,$$

*Mais il y une façon plus simple de procéder ! La clé réside dans le fait que $J(2^m) = 1$ pour tout $m$, ce qui se déduit immédiatement de notre première équation, $J(2n) = 2J(n) - 1$. Nous savons donc que la première personne survit chaque fois que $n$ est une puissance de 2. Dans le cas général, quand $n = 2^m + l$, le nombre de personnes devient une puissance de 2 dès qu'il y a eu $l$ exécutions. La première personne, parmi celles qui restent à ce moment-là, porte le numéro $2l + 1$.*

où chaque $b_i$ a pour valeur 0 ou 1, et le premier bit $b_m$ est égal à 1. sachant que $n = 2^m + l$, on a, successivement,

$$\begin{aligned} n &= (1\, b_{m-1}\, b_{m-2} \ldots b_1\, b_0)_2\,, \\ l &= (0\, b_{m-1}\, b_{m-2} \ldots b_1\, b_0)_2\,, \\ 2l &= (b_{m-1}\, b_{m-2} \ldots b_1\, b_0\, 0)_2\,, \\ 2l+1 &= (b_{m-1}\, b_{m-2} \ldots b_1\, b_0\, 1)_2\,, \\ J(n) &= (b_{m-1}\, b_{m-2} \ldots b_1\, b_0\, b_m)_2\,. \end{aligned}$$

(La dernière ligne provient du fait que $J(n) = 2l + 1$ et $b_m = 1$). Nous avons donc prouvé que

$$J\big((b_m\, b_{m-1} \ldots b_1\, b_0)_2\big) = (b_{m-1} \ldots b_1\, b_0\, b_m)_2\,. \tag{1.10}$$

Un informaticien dirait qu'on trouve $J(n)$ à partir de $n$ en effectuant un décalage circulaire d'un bit vers la gauche. C'est magique ! Par exemple, si $n = 100 = (1100100)_2$, alors $J(n) = J\big((1100100)_2\big) = (1001001)_2$, ce qui fait $64 + 8 + 1 = 73$. Si nous avions travaillé en représentation binaire depuis le début, nous aurions probablement immédiatement remarqué ce fait.

*(Ici, "itérer" signifie appliquer une fonction sur elle-même).*

Si on itère la fonction $J$ $m + 1$ fois en partant de $n$ , on effectue $m + 1$ décalages circulaires d'un bit. Puisque $n$ s'écrit avec $(m+1)$ bits, on devrait donc s'attendre à trouver $n$ ; mais ça ne marche pas. Par exemple, si $n = 13$, on a $J\big((1101)_2\big) = (1011)_2$ ; mais alors $J\big((1011)_2\big) = (111)_2$ et le processus se détraque : le 0 disparaît lorsqu'il arrive en première position. En fait, comme $J(n)$ est le numéro du survivant, il est $\leqslant n$ par définition ; donc, si $J(n) < n$, on ne peut jamais retrouver $n$ en continuant à itérer.

En appliquant $J$ de façon répétée, on obtient une suite décroissante de valeurs qui finit par atteindre un "point fixe" pour lequel $J(n) = n$. On voit facilement ce que sera ce point fixe, grâce à une propriété évidente de notre décalage circulaire : en itérant la fonction un nombre suffisant de fois, on obtient toujours un nombre représenté par une suite de 1 ; ce nombre a pour valeur $2^{\nu(n)} - 1$, où $\nu(n)$ est le nombre de chiffres 1 dans la représentation binaire de $n$. Ainsi, comme $\nu(13) = 3$, on obtient

*Curieusement, si $M$ est une $n$-variété $C^\infty$ compacte ($n > 1$), il existe un plongement différentiable de $M$ dans $\mathbf{R}^{2n-\nu(n)}$, mais pas nécessairement dans $\mathbf{R}^{2n-\nu(n)-1}$. Je me demande si Josèphe n'était pas un topologiste ignoré.*

$$\overbrace{J(J(\ldots J}^{\text{au moins deux } J}(13)\ldots)) = 2^3 - 1 = 7;$$

de la même façon,

$$\overbrace{J(J(\ldots J}^{\text{au moins 8}}((101101101101011)_2)\ldots)) = 2^{10} - 1 = 1023.$$

Incroyable mais vrai.

Revenons brièvement à notre première conjecture : $J(n) = n/2$ lorsque $n$ est pair. C'est évidemment faux en général, mais nous pouvons maintenant déterminer dans quels cas c'est vrai : $J(n) = n/2$, $2l+1 = (2^m + l)/2$, $l = \frac{1}{3}(2^m - 2)$. Si le nombre $l = \frac{1}{3}(2^m - 2)$ est entier, alors $n = 2^m + l$ est une solution car $l$ est plus petit que $2^m$. Il est facile de vérifier que $2^m - 2$ est un multiple de 3 lorsque $m$ est impair, mais pas quand il est pair (nous étudierons des problèmes de ce genre au chapitre 4). Il y a donc une infinité de solutions à l'équation $J(n) = n/2$. Voici les premières :

| $m$ | $l$ | $n = 2^m + l$ | $J(n) = 2l + 1 = n/2$ | $n$ (en base 2) |
|---|---|---|---|---|
| 1 | 0 | 2 | 1 | 10 |
| 3 | 2 | 10 | 5 | 1010 |
| 5 | 10 | 42 | 21 | 101010 |
| 7 | 42 | 170 | 85 | 10101010 |

Remarquez que la dernière colonne est constituée des nombres binaires pour lesquels un décalage circulaire d'un chiffre vers la gauche produit le même effet qu'un décalage ordinaire d'un chiffre vers la droite (division par 2).

Maintenant que nous connaissons extrêmement bien la fonction $J$, il s'agit de la généraliser. Que se serait-il passé si nous avions dû résoudre une récurrence du genre de (1.8), mais avec des constantes différentes ? Nous n'aurions probablement pas pu deviner la solution, car elle doit être plutôt étrange. Voyons cela de plus près en introduisant des constantes $\alpha$, $\beta$ et $\gamma$ et en cherchant une forme close pour la récurrence plus générale

*Pour moi, c'est comme si c'était du grec.*

$$\begin{aligned} f(1) &= \alpha; \\ f(2n) &= 2f(n) + \beta, \qquad \text{pour } n \geqslant 1; \\ f(2n+1) &= 2f(n) + \gamma, \qquad \text{pour } n \geqslant 1. \end{aligned} \tag{1.11}$$

(Dans la récurrence d'origine, nous avions $\alpha = 1$, $\beta = -1$ et $\gamma = 1$). Avec cette récurrence, on peut construire le tableau suivant :

| $n$ | $f(n)$ |
|---|---|
| 1 | $\alpha$ |
| 2 | $2\alpha + \beta$ |
| 3 | $2\alpha + \gamma$ |
| 4 | $4\alpha + 3\beta$ |
| 5 | $4\alpha + 2\beta + \gamma$ |
| 6 | $4\alpha + \beta + 2\gamma$ |
| 7 | $4\alpha + 3\gamma$ |
| 8 | $8\alpha + 7\beta$ |
| 9 | $8\alpha + 6\beta + \gamma$ |

(1.12)

Les coefficients de $\alpha$ semblent bien être les plus grandes puissances de 2 inférieures ou égales à $n$. De plus, entre deux puissances de 2 consécutives, les coefficients de $\beta$ décroissent de 1 en 1 jusqu'à 0, tandis que ceux de $\gamma$ croissent de 1 en 1 à partir de 0. Donc, si on écrit $f(n)$ sous la forme

$$f(n) = A(n)\alpha + B(n)\beta + C(n)\gamma \tag{1.13}$$

pour distinguer ce qui dépend de $\alpha$, $\beta$ et $\gamma$, il semble que

$$\begin{aligned} A(n) &= 2^m; \\ B(n) &= 2^m - 1 - l; \\ C(n) &= l, \end{aligned} \tag{1.14}$$

où, comme d'habitude, $n = 2^m + l$ et $0 \leqslant l < 2^m$, pour $n \geqslant 1$.

*Accrochez-vous, ce qui va suivre est nouveau.*

Il n'est pas extrêmement difficile de prouver (1.13) et (1.14) par induction, mais les calculs ne sont pas très propres et ne nous apprennent rien. Il y a heureusement une meilleure façon de procéder : il s'agit de choisir des valeurs particulières et de les combiner entre elles. Illustrons ceci en considérant le cas particulier $\alpha = 1$, $\beta = \gamma = 0$. La fonction $f(n)$ est donc supposée égale à $A(n)$, et la récurrence (1.11) devient

$$\begin{aligned} A(1) &= 1; \\ A(2n) &= 2A(n), \qquad \text{pour } n \geqslant 1; \\ A(2n+1) &= 2A(n), \qquad \text{pour } n \geqslant 1. \end{aligned}$$

On en déduit facilement, par induction sur $m$, que $A(2^m + l) = 2^m$.

Maintenant, nous allons utiliser la récurrence (1.11) et la solution (1.13) *à l'envers*, en partant d'une fonction $f(n)$ et en regardant s'il existe des constantes $(\alpha, \beta, \gamma)$ qui permettent de la définir. En injectant la fonction constante $f(n) = 1$ dans (1.11), on trouve

*Bonne idée !*

$$\begin{aligned} 1 &= \alpha; \\ 1 &= 2\cdot 1 + \beta; \\ 1 &= 2\cdot 1 + \gamma. \end{aligned}$$

La solution de ce système est le triplet $(\alpha, \beta, \gamma) = (1, -1, -1)$ ; ainsi, $A(n) - B(n) - C(n) = f(n) = 1$. On peut de la même manière injecter $f(n) = n$ dans (1.11) :

$$\begin{aligned} 1 &= \alpha; \\ 2n &= 2\cdot n + \beta; \\ 2n+1 &= 2\cdot n + \gamma; \end{aligned}$$

Ces équations sont vérifiées pour tout $n$ si $\alpha = 1$, $\beta = 0$ et $\gamma = 1$ ; inutile donc de prouver par induction que, avec ces valeurs pour les paramètres $\alpha$,

$\beta$ et $\gamma$, $f(n)$ sera égal à $n$. Nous *savons* déjà que la solution sera $f(n) = n$ dans ce cas, car la récurrence (1.11) définit $f(n)$ de façon unique pour toute valeur de $n$.

C'est quasiment terminé ! Nous avons montré que les fonctions $A(n)$, $B(n)$ et $C(n)$ de (1.13), qui donnent la solution générale de (1.11), satisfont les équations

$$\begin{aligned} A(n) &= 2^m, \qquad \text{où } n = 2^m + l \text{ et } 0 \leqslant l < 2^m; \\ A(n) - B(n) - C(n) &= 1; \\ A(n) + C(n) &= n. \end{aligned}$$

*Attention : les auteurs espèrent nous donner une idée de la méthode du répertoire en nous la présentant sur des cas d'école au lieu de nous la décrire de façon structurée. Cette méthode marche le mieux avec les récurrences "linéaires", c'est-à-dire les récurrences dont les solutions peuvent s'exprimer comme une somme de produits de certains paramètres par des fonctions de $n$, comme dans l'équation (1.13). La formule-clé est (1.13).*

Nos conjectures de (1.14) s'ensuivent immédiatement, du fait qu'en résolvant ces équations on trouve $C(n) = n - A(n) = l$ et $B(n) = A(n) - 1 - C(n) = 2^m - 1 - l$.

Cette approche est une illustration d'une méthode étonnamment utile pour résoudre des récurrences, la *méthode du répertoire*. Il s'agit d'abord de trouver des valeurs des paramètres pour lesquelles la solution est connue. On constitue ainsi un répertoire de cas particuliers que l'on sait résoudre. On résout alors le cas général en combinant ces cas particuliers. Il faut utiliser autant de cas particuliers indépendants que le nombre de paramètres du cas général (ici trois, pour $\alpha$, $\beta$ and $\gamma$). Les exercices 16 et 20 donnent d'autres exemples de la méthode du répertoire.

Revenons à la récurrence d'origine. Nous savons qu'elle a une solution magique en base 2 :

$$J\big((b_m\, b_{m-1} \ldots b_1\, b_0)_2\big) = (b_{m-1} \ldots b_1\, b_0\, b_m)_2\,, \qquad \text{où } b_m = 1.$$

La récurrence de Josèphe généralisée possède-t-elle aussi cette magie ?

Bien sûr ! Pourquoi pas ? On peut réécrire la récurrence généralisée (1.11) ainsi :

$$\begin{aligned} f(1) &= \alpha; \\ f(2n + j) &= 2f(n) + \beta_j\,, \qquad \text{pour } j = 0, 1 \quad \text{et} \quad n \geqslant 1, \end{aligned} \tag{1.15}$$

en posant $\beta_0 = \beta$ et $\beta_1 = \gamma$. En développant cette récurrence en mode binaire, on obtient

$$\begin{aligned} f\big((b_m\, b_{m-1} \ldots b_1\, b_0)_2\big) &= 2f\big((b_m\, b_{m-1} \ldots b_1)_2\big) + \beta_{b_0} \\ &= 4f\big((b_m\, b_{m-1} \ldots b_2)_2\big) + 2\beta_{b_1} + \beta_{b_0} \\ &\;\;\vdots \\ &= 2^m f\big((b_m)_2\big) + 2^{m-1}\beta_{b_{m-1}} + \cdots + 2\beta_{b_1} + \beta_{b_0} \\ &= 2^m\alpha + 2^{m-1}\beta_{b_{m-1}} + \cdots + 2\beta_{b_1} + \beta_{b_0}\,. \end{aligned}$$

*("relâcher" = "détruire")*

Supposons qu'on relâche les contraintes de l'écriture en base 2 pour autoriser n'importe quel chiffre, au lieu de 0 et 1 seulement. On déduit du calcul précédent que

$$f\big((b_m\, b_{m-1} \ldots b_1\, b_0)_2\big) \;=\; (\alpha\, \beta_{b_{m-1}}\, \beta_{b_{m-2}} \ldots \beta_{b_1}\, \beta_{b_0})_2\,. \qquad (1.16)$$

Bien. Nous aurions pu voir cela plus tôt si nous avions écrit (1.12) d'une autre manière :

*Je crois que j'ai compris : les représentations binaires de $A(n)$, $B(n)$ et $C(n)$ ont leurs 1 dans des positions différentes.*

| $n$ | $f(n)$ |
|---|---|
| 1 | $\alpha$ |
| 2 | $2\alpha + \beta$ |
| 3 | $2\alpha + \gamma$ |
| 4 | $4\alpha + 2\beta + \beta$ |
| 5 | $4\alpha + 2\beta + \gamma$ |
| 6 | $4\alpha + 2\gamma + \beta$ |
| 7 | $4\alpha + 2\gamma + \gamma$ |

Par exemple, lorsque $n = 100 = (1100100)_2$, en prenant les valeurs d'origine $\alpha = 1$, $\beta = -1$ et $\gamma = 1$, on obtient

$$\begin{array}{rcccccccccc} n = & (\,1 & 1 & 0 & 0 & 1 & 0 & 0\,)_2 & = & 100 \\ \hline f(n) = & (\,1 & 1 & -1 & -1 & 1 & -1 & -1\,)_2 & & \\ = & +64 & +32 & -16 & -8 & +4 & -2 & -1 & = & 73 \end{array}$$

comme auparavant. La propriété du décalage circulaire se déduit du fait que chaque bloc de chiffres binaires $(1\,0 \ldots 0\,0)_2$ de la représentation de $n$ se transforme en

$$(1\,{-1} \ldots {-1}\,{-1})_2 \;=\; (0\,0 \ldots 0\,1)_2\,.$$

*"There are two kinds of generalizations. One is cheap and the other is valuable. It is easy to generalize by diluting a little idea with a big terminology. It is much more difficult to prepare a refined and condensed extract from several good ingredients."*
*—G. Pólya [297]*

Ainsi, en changeant de notation nous avons trouvé la solution compacte (1.16) de la récurrence générale (1.15). On peut même se permettre de généraliser plus encore. La récurrence

$$\begin{aligned} f(j) &= \alpha_j\,, && \text{pour } 1 \leqslant j < d; \\ f(dn + j) &= cf(n) + \beta_j\,, && \text{pour } 0 \leqslant j < d \quad \text{et} \quad n \geqslant 1, \end{aligned} \qquad (1.17)$$

est la même que la précédente, sauf qu'on part de nombres en base d pour produire des nombres en base c. Ainsi, la solution, avec changement de base, est

$$f\big((b_m\, b_{m-1} \ldots b_1\, b_0)_d\big) \;=\; (\alpha_{b_m}\, \beta_{b_{m-1}}\, \beta_{b_{m-2}} \ldots \beta_{b_1}\, \beta_{b_0})_c\,. \qquad (1.18)$$

Supposons par exemple que, par chance, on nous donne la récurrence

*Ou peut-être par mal chance.*

$$\begin{aligned} f(1) &= 34\,, \\ f(2) &= 5\,, \\ f(3n) &= 10f(n)+76\,, \qquad \text{pour } n \geqslant 1, \\ f(3n+1) &= 10f(n)-2\,, \qquad \text{pour } n \geqslant 1, \\ f(3n+2) &= 10f(n)+8\,, \qquad \text{pour } n \geqslant 1, \end{aligned}$$

pour calculer $f(19)$. Ici, on a $d = 3$ et $c = 10$. Nous savons que $19 = (201)_3$, et la solution avec changement de base nous indique qu'il faut effectuer un remplacement chiffre par chiffre, en passant de la base 3 vers la base 10. Ainsi, le 2 devient un 5, et les 0 et 1 se transforment respectivement en 76 et $-2$, pour donner la réponse :

$$f(19) = f\big((201)_3\big) = (5\ 76\ {-2})_{10} = 1258\,,$$

Ainsi, Josèphe et la guerre entre Rome et les Juifs nous ont amenés à rencontrer quelques récurrences générales intéressantes.

*Je suis contre les guerres récurrentes.*

## Exercices

### *Echauffements*

**1** Tous les chevaux ont la même couleur ; on peut le prouver par induction sur le nombre de chevaux d'un ensemble donné. Voici comment : "s'il n'y a qu'un cheval, il est de la même couleur que lui-même, donc la base est triviale. Pour l'étape d'induction, supposons qu'il y a $n$ chevaux numérotés de 1 à $n$. De par l'hypothèse d'induction, les chevaux 1 à $n-1$ sont de la même couleur et les chevaux de 2 à $n$ sont de la même couleur. Cependant, les chevaux numérotés de 2 à $n-1$ ne peuvent pas changer de couleur en changeant de groupe ; ce sont des chevaux, non des caméléons. Donc, par transitivité, les chevaux de 1 à $n$ doivent tous être de la même couleur. Ainsi les $n$ chevaux ont tous la même couleur. CQFD." Qu'est-ce qui cloche dans ce raisonnement ?

*Vous êtes priés de faire tous les échauffements de tous les chapitres !*
*— La Directio.*

**2** Trouver la plus courte suite de mouvements pour transférer une tour de $n$ disques de l'axe de gauche A vers l'axe de droite B, si on interdit les transferts directs entre A et B (on ne peut effectuer un mouvement que depuis ou vers l'axe du milieu). Comme d'habitude, on ne peut pas poser un disque sur un disque plus petit.

**3** Montrer que, au cours du transfert d'une tour sous les hypothèses de l'exercice précédent, on va rencontrer toutes les configurations possibles de $n$ disques convenablement empilés sur trois axes.