Ainsi, dans le cas déjà connu où $q = 2$, D croît jusqu'à 2^{m+1} lorsque $l = 2^m + l$; donc $J_2(n) = 2(2^m + l) + 1 - 2^{m+1} = 2l + 1$. Parfait.

Avec la recette de (3.19), on calcule une suite d'entiers qui peut être définie par la récurrence suivante :

$$\begin{aligned} D_0^{(q)} &= 1\,; \\ D_n^{(q)} &= \left\lceil \frac{q}{q-1} D_{n-1}^{(q)} \right\rceil \qquad \text{pour } n > 0. \end{aligned} \tag{3.20}$$

Apparemment, ces nombres ne sont pas liés à des fonctions connues, sauf lorsque $q = 2$; ils n'ont donc probablement pas de jolie forme close. Cependant, si on considère comme "connue" la suite $D_n^{(q)}$, alors on peut facilement décrire la solution du problème de Josèphe généralisé : le survivant $J_q(n)$ est $qn + 1 - D_k^{(q)}$, où k est le plus petit entier tel que $D_k^{(q)} > (q-1)n$.

"Connue" comme, par exemple, la suite des nombres harmoniques. A.M. Odlyzko et H.S. Wilf ont montré [283] que $D_n^{(3)} = \lfloor (\frac{3}{2})^n C \rfloor$, où $C \approx 1,6222705$.

3.4 "MOD" : L'OPÉRATION BINAIRE

Si m et n sont des entiers strictement positifs, le quotient de la division de n par m est $\lfloor n/m \rfloor$. Le reste de cette division est noté "$n \bmod m$". La formule de base

$$n = m \underbrace{\lfloor n/m \rfloor}_{\text{quotient}} + \underbrace{n \bmod m}_{\text{reste}}$$

indique que $n \bmod m$ est égal à $n - m\lfloor n/m \rfloor$. Ceci peut être généralisé aux entiers négatifs, et même à tous les nombres réels :

$$x \bmod y = x - y\lfloor x/y \rfloor\,, \qquad \text{pour } y \neq 0. \tag{3.21}$$

Ainsi, "mod" est une opération binaire, tout comme l'addition et la soustraction. Les mathématiciens utilisent mod ainsi depuis longtemps, en manipulant des nombres mod 10 ou mod 2π par exemple ; mais cette notion n'est formellement définie que depuis une vingtaine d'années. Vieille notion, jeune notation.

Pourquoi appellent-ils mod "l'opération binaire" ? Réponse dans le passionnant prochain chapitre.

La signification intuitive de $x \bmod y$ est facile à saisir lorsque x et y sont des entiers positifs. Imaginons un cercle de circonférence y dont les points représentent les nombres réels de l'intervalle $[0\,..\,y)$. Si on suit la circonférence sur une distance x en partant de 0, le point où on s'arrête est $x \bmod y$ (et le nombre de fois qu'on est passé au point 0 est égal à $\lfloor x/y \rfloor$).

Si l'un des nombres x ou y est négatif, il faut étudier de plus près la définition pour voir exactement ce qu'elle signifie. Voici quelques exemples :

Attention, certains langages informatiques utilisent une définition différente.

$$5 \bmod 3 = 5 - 3\lfloor 5/3 \rfloor \qquad = 2\,;$$

$$\begin{aligned} 5 \bmod -3 &= 5-(-3)\lfloor 5/(-3)\rfloor &&= -1\,; \\ -5 \bmod 3 &= -5-3\lfloor -5/3\rfloor &&= 1\,; \\ -5 \bmod -3 &= -5-(-3)\lfloor -5/(-3)\rfloor &&= -2\,. \end{aligned}$$

Que diriez-vous de l'appeler le modumeur ?

Le nombre situé après "mod" est appelé le *module* ; personne n'a encore donné un nom au nombre avant "mod". En pratique, le module est généralement positif, mais la définition garde tout son sens quand il est négatif. Dans les deux cas, la valeur de $x \bmod y$ est entre 0 et le module :

$$\begin{aligned} 0 \leqslant x \bmod y &< y\,, \qquad \text{pour } y > 0; \\ 0 \geqslant x \bmod y &> y\,, \qquad \text{pour } y < 0. \end{aligned}$$

Que se passe-t-il si $y = 0$? Pour éviter de diviser par 0, ce cas a été évité dans la définition (3.21). Toutefois, pour être complet, on peut convenir que

$$x \bmod 0 = x\,. \tag{3.22}$$

Ainsi on préserve le fait que la différence entre $x \bmod y$ et x est un multiple de y. (Il pourrait sembler plus naturel de faire en sorte que la fonction soit continue en 0 en posant $x \bmod 0 = \lim_{y\to 0} x \bmod y = 0$; mais nous verrons au chapitre 4 que ce serait moins intéressant. La continuité n'est pas un élément très important dans l'opération mod).

Nous avons déjà vu, dans une version déguisée, un cas particulier de mod : lorsque nous avons écrit x en fonction de ses parties entière et fractionnaire, $x = \lfloor x\rfloor + \{x\}$. La partie fractionnaire peut aussi s'écrire $x \bmod 1$ car on a

$$x = \lfloor x\rfloor + x \bmod 1\,.$$

Notez qu'on n'a pas besoin de mettre des parenthèses dans cette formule : on considère que mod est prioritaire face à l'addition ou à la soustraction.

Pour définir mod, nous avons fait appel à la partie entière inférieure. La partie entière supérieure doit légitimement se sentir frustrée. Peut-être pourrait-on l'utiliser pour définir un analogue de mod, comme ceci :

A un moment dans les années 70, il fallait être "mod" pour être à la mode. Peut-être qu'on pourrait rebaptiser "punk" cette fonction marmot ?

Non ! j'aime "marmot".

$$x \operatorname{marmot} y = y\lceil x/y\rceil - x\,.$$

Dans le cercle défini plus haut, cela représente la distance qui reste à parcourir pour atteindre le point 0 après avoir parcouru une distance x. Bien entendu, il faudrait trouver un terme plus adéquat que "marmot". Si nous trouvons des applications pratiques de cette opération, il est probable qu'un terme approprié surgira naturellement.

La propriété algébrique la plus importante de mod est sa distributivité : on a

$$c(x \bmod y) \;=\; (cx) \bmod (cy) \tag{3.23}$$

pour tous réels c, x et y. (Ceux qui considèrent que la multiplication est prioritaire par rapport à mod peuvent ôter les parenthèses du membre de droite). Cette loi est facile à prouver à partir de la définition (3.21), car

$$c(x \bmod y) \;=\; c(x - y\lfloor x/y \rfloor) \;=\; cx - cy\lfloor cx/cy \rfloor \;=\; cx \bmod cy$$

si $cy \neq 0$, et la formule est trivialement vraie si le module est nul. Si on prend $c = -1$, la distributivité est illustrée deux fois dans nos quatre exemples avec ± 5 et ± 3. L'identité (3.23) est rassurante, en ce sens qu'elle nous donne des raisons de penser que "mod" n'a pas été indûment définie.

Dans le reste de cette section, nous allons voir une application pratique dans laquelle "mod" est fort utile, bien que ne jouant pas un rôle de premier plan. Ce problème arrive couramment dans des situations variées : on veut répartir n objets en m groupes aussi égaux que possible.

Ah oui, le reste. Ha ! ha !

Supposons par exemple que nous voulions mettre en page n courtes lignes de texte dans m colonnes. Pour des raisons d'esthétique, nous voulons que les colonnes soient positionnées dans l'ordre des longueurs décroissantes. De plus, les longueurs des colonnes doivent être à peu près égales : les longueurs de deux colonnes distinctes ne doivent pas différer de plus d'une ligne de texte. Par exemple, s'il faut diviser 37 lignes de texte en cinq colonnes, on préférera la disposition de droite :

8	8	8	8	5
ligne 1	ligne 9	ligne 17	ligne 25	ligne 33
ligne 2	ligne 10	ligne 18	ligne 26	ligne 34
ligne 3	ligne 11	ligne 19	ligne 27	ligne 35
ligne 4	ligne 12	ligne 20	ligne 28	ligne 36
ligne 5	ligne 13	ligne 21	ligne 29	ligne 37
ligne 6	ligne 14	ligne 22	ligne 30	
ligne 7	ligne 15	ligne 23	ligne 31	
ligne 8	ligne 16	ligne 24	ligne 32	

8	8	7	7	7
ligne 1	ligne 9	ligne 17	ligne 24	ligne 31
ligne 2	ligne 10	ligne 18	ligne 25	ligne 32
ligne 3	ligne 11	ligne 19	ligne 26	ligne 33
ligne 4	ligne 12	ligne 20	ligne 27	ligne 34
ligne 5	ligne 13	ligne 21	ligne 28	ligne 35
ligne 6	ligne 14	ligne 22	ligne 29	ligne 36
ligne 7	ligne 15	ligne 23	ligne 30	ligne 37
ligne 8	ligne 16			

En outre, si on considère que les lignes sont numérotées, on veut que deux lignes successives d'une même colonne aient des numéros successifs, car c'est dans ce sens qu'on lit en général. Il faudra donc d'abord décider combien de lignes iront dans la première colonne, puis considérer la deuxième colonne, puis la troisième et ainsi de suite. Si on distribuait les lignes rangée par rangée, on aurait un bon nombre de lignes dans chaque colonne, mais l'ordre des lignes serait incorrect (on obtiendrait quelque chose ressemblant à la disposition de droite, mais la colonne 1 contiendrait les lignes 1, 6, 11, ..., 36 au lieu de 1, 2, 3, ... 8).

On ne peut donc utiliser une stratégie de rangement "rangée par rangée". Cependant cette stratégie peut quand même nous indiquer combien

il faut mettre de lignes dans chaque colonne. Si n n'est pas un multiple de m, il est clair que cette procédure aurait pour résultat de mettre $\lceil n/m \rceil$ lignes dans les colonnes les plus longues et $\lfloor n/m \rfloor$ lignes dans les courtes (et il y aurait exactement n marmot m colonnes courtes).

Pour généraliser notre propos, parlons dorénavant d'"objets" et de "groupes" plutôt que de "lignes" et de "colonnes". Nous venons de décider que le premier groupe contiendrait $\lceil n/m \rceil$ objets. Pour distribuer séquentiellement n objets dans m urnes (avec $m > 0$), on doit donc pouvoir appliquer le plan suivant : mettre $\lceil n/m \rceil$ objets dans un groupe, puis appliquer récursivement la même procédure pour ranger les $n' = n - \lceil n/m \rceil$ objets restant dans les $m' = m - 1$ groupes restant.

Par exemple, si $n = 314$ et $m = 6$, la distribution évolue de la manière suivante :

objets restant	groupes restant	$\lceil$objets/groupe$\rceil$
314	6	53
261	5	53
208	4	52
156	3	52
104	2	52
52	1	52

Ça marche. On obtient bien des groupes de taille à peu près égale, même si le diviseur varie au cours du temps.

Au fait, pourquoi est-ce que ça marche ? Posons $n = qm + r$, où $q = \lfloor n/m \rfloor$ et $r = n \bmod m$. Si $r = 0$, le procédé est simple : on met $\lceil n/m \rceil = q$ objets dans le premier groupe et on remplace n par $n' = n - q$. Il reste alors $n' = qm'$ objets à ranger dans $m' = m - 1$ groupes. D'autre part, si $r > 0$, on met $\lceil n/m \rceil = q + 1$ objets dans le premier groupe et on remplace n par $n' = n - q - 1$, ce qui laisse $n' = qm' + r - 1$ objets à répartir dans les autres groupes. Le nouveau reste est $r' = r - 1$, mais q est inchangé. Il s'ensuit qu'il y aura r groupes de $q + 1$ objets suivis de $m - r$ groupes de q objets.

Combien y a-t-il d'objets dans le kième groupe ? Il nous faudrait une formule donnant $\lceil n/m \rceil$ si $k \leqslant n \bmod m$ et $\lfloor n/m \rfloor$ sinon. Il n'est pas difficile de voir que

$$\left\lceil \frac{n - k + 1}{m} \right\rceil$$

convient, car c'est égal à $q + \lceil (r - k + 1)/m \rceil$ si on écrit, comme dans le paragraphe précédent, $n = qm + r$, avec $q = \lfloor n/m \rfloor$. On sait que $\lceil (r - k + 1)/m \rceil = [k \leqslant r]$ si $1 \leqslant k \leqslant m$ et $0 \leqslant r < m$. Nous pouvons donc donner une identité qui décrit la partition de n en m parts "les plus égales

possibles" :

$$n = \left\lceil \frac{n}{m} \right\rceil + \left\lceil \frac{n-1}{m} \right\rceil + \cdots + \left\lceil \frac{n-m+1}{m} \right\rceil . \tag{3.24}$$

Cette identité est valable pour tout entier strictement positif m et pour tout entier n (positif, négatif ou nul). Nous avons déjà rencontré le cas $m = 2$ en (3.17) sous une forme un peu différente : $n = \lceil n/2 \rceil + \lfloor n/2 \rfloor$.

Si nous avions voulu que les parts soient en ordre de tailles décroissantes nous aurons procédé de manière similaire, la seule différence étant que nous aurions mis $\lfloor n/m \rfloor$ objets dans le premier groupe. Nous aurions alors trouvé l'identité correspondante :

$$n = \left\lfloor \frac{n}{m} \right\rfloor + \left\lfloor \frac{n+1}{m} \right\rfloor + \cdots + \left\lfloor \frac{n+m-1}{m} \right\rfloor . \tag{3.25}$$

On peut passer de (3.25) à (3.24) et réciproquement en utilisant, au choix, (3.4) ou l'identité de l'exercice 12.

Maintenant, en remplaçant le n de (3.25) par $\lfloor mx \rfloor$ et en appliquant la règle (3.11) pour supprimer les parties entières à l'intérieur d'autres parties entières, on obtient une identité valable pour tout réel x :

$$\lfloor mx \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{m} \right\rfloor + \cdots + \left\lfloor x + \frac{m-1}{m} \right\rfloor . \tag{3.26}$$

C'est assez étonnant. En effet, nous savons bien que la fonction partie entière inférieure donne une approximation entière d'une valeur réelle ; mais ce qui se passe ici, c'est que l'unique approximation de gauche donne le même résultat que la somme des approximations de droite. Si on considère que $\lfloor x \rfloor$ est en moyenne à peu près égal à $x - \frac{1}{2}$, le membre de gauche vaut à peu près $mx - \frac{1}{2}$, tandis que celui de droite donne, en gros, $(x - \frac{1}{2}) + (x - \frac{1}{2} + \frac{1}{m}) + \cdots + (x - \frac{1}{2} + \frac{m-1}{m}) = mx - \frac{1}{2}$; et il se trouve que la somme de toutes ces approximations grossières est exacte !

3.5 SOMMES DE PARTIES ENTIÈRES

L'équation (3.26) montre qu'il existe au moins un type de sommes contenant des $\lfloor\ \rfloor$ pour lesquelles on peut trouver une formule close. Est-ce possible pour d'autres sommes ? La réponse est oui. Il y a un truc qui marche généralement dans ce genre de cas : se débarrasser des parties entières en introduisant une nouvelle variable.

Par exemple, voyons s'il est possible de trouver une formule close pour la somme

$$\sum_{0 \leqslant k < n} \lfloor \sqrt{k} \rfloor .$$

Par exemple, si $m = 41$ et $n = 127$, la somme de gauche contient 41 termes tandis que celle de droite en a 127 ; et pourtant, elles sont égales pour tout réel x.

Exercices

Echauffements

1 Au cours de l'analyse du problème de Josèphe au chapitre 1, nous avons décidé d'écrire un entier n quelconque sous la forme $n = 2^m + l$, où $0 \leqslant l < 2^m$. Calculez explicitement l et m en fonction de n, en utilisant les crochets de partie entière inférieure et/ou supérieure.

2 Trouvez une formule qui donne l'entier le plus proche d'un nombre réel donné x. Si x se trouve exactement au milieu de deux entiers, donnez une expression qui arrondit (a) par excès ; (b) par défaut.

3 Calculez $\lfloor \lfloor m\alpha \rfloor n/\alpha \rfloor$, où m et n sont des entiers strictement positifs et α un nombre irrationnel supérieur à n.

4 On définit dans ce chapitre les problèmes de niveau 1 à 5. Qu'est-ce qu'un problème de niveau 0 ? (Celui-ci n'est *pas* un problème de niveau 0).

5 Donnez une condition nécessaire et suffisante pour que $\lfloor nx \rfloor = n\lfloor x \rfloor$ lorsque n est un entier strictement positif. (On a le droit d'utiliser $\{x\}$ dans la condition).

6 Peut-on dire quelque chose d'intéressant sur $\lfloor f(x) \rfloor$ quand $f(x)$ est une fonction continue et strictement *décroissante* dont la valeur ne peut être entière que si x est un entier ?

7 Résolvez la récurrence

$$\begin{aligned} X_n &= n\,, && \text{pour } 0 \leqslant n < m; \\ X_n &= X_{n-m} + 1\,, && \text{pour } n \geqslant m. \end{aligned}$$

8 Démontrez le *principe des boîtes de Dirichlet* : si on range n objets dans m boîtes, il y a au moins une boîte qui contient $\geqslant \lceil n/m \rceil$ objets, et au moins une boite qui en contient $\leqslant \lfloor n/m \rfloor$.

Comment sait-on si on est à l'université ? C'est quand votre livre ne vous dit pas comment on doit prononcer "Dirichlet".

9 En 1800 avant Jésus-Christ, les mathématiciens égyptiens représentaient les nombres rationnels entre 0 et 1 comme des sommes de fractions unitaires $1/x_1 + \cdots + 1/x_k$, où les x_i étaient des entiers strictement positifs distincts. Par exemple, ils écrivaient $\frac{1}{3} + \frac{1}{15}$ au lieu de $\frac{2}{5}$. Montrez qu'on peut toujours le faire de façon systématique : si $0 < m/n < 1$, alors

$$\frac{m}{n} = \frac{1}{q} + \left\{\text{représentation de } \frac{m}{n} - \frac{1}{q}\right\}, \qquad q = \left\lceil \frac{n}{m} \right\rceil .$$

(C'est l'*algorithme de Fibonacci*, dû à Leonardo Fibonacci (1202)).

Exercices de base

10 Montrez que l'expression

$$\left\lceil \frac{2x+1}{2} \right\rceil - \left\lceil \frac{2x+1}{4} \right\rceil + \left\lfloor \frac{2x+1}{4} \right\rfloor$$

est toujours égale soit à $\lfloor x \rfloor$, soit à $\lceil x \rceil$. Dans quelles circonstances chacun de ces cas se produit-il ?

11 Ecrivez en détail la preuve, éludée dans le chapitre, du fait que l'intervalle ouvert $(\alpha \mathinner{..} \beta)$ contient exactement $\lceil \beta \rceil - \lfloor \alpha \rfloor - 1$ entiers lorsque $\alpha < \beta$. Pourquoi la preuve ne peut-elle être correcte que si on exclut le cas $\alpha = \beta$?

12 Montrez que

$$\left\lceil \frac{n}{m} \right\rceil = \left\lfloor \frac{n+m-1}{m} \right\rfloor$$

pour tout entier n et tout entier strictement positif m. (Cette identité nous fournit une nouvelle méthode, différente de la règle (3.4), pour convertir des parties entières supérieures en parties entières inférieures et vice-versa).

13 Soient α et β deux réels strictement positifs. Montrez que $\mathrm{Spec}(\alpha)$ et $\mathrm{Spec}(\beta)$ forment une partition de l'ensemble des entiers strictement positifs si et seulement si α et β sont irrationnels et $1/\alpha + 1/\beta = 1$.

14 Prouvez ou réfutez l'égalité suivante :

$$(x \bmod ny) \bmod y \;=\; x \bmod y\,, \qquad n \text{ entier.}$$

15 Existe-t-il une identité analogue à (3.26) faisant intervenir des parties entières inférieures au lieu de parties entières supérieures ?

16 Montrez que $n \bmod 2 = \bigl(1 - (-1)^n\bigr)/2$. Trouvez et prouvez une expression similaire pour $n \bmod 3$, de la forme $a + b\omega^n + c\omega^{2n}$, où ω est le nombre complexe $(-1 + i\sqrt{3})/2$. *Suggestion :* remarquez que $\omega^3 = 1$ et $1 + \omega + \omega^2 = 0$.

17 Calculez la somme $\sum_{0 \leqslant k < m} \lfloor x + k/m \rfloor$ dans le cas où $x \geqslant 0$, en substituant $\sum_j [1 \leqslant j \leqslant x + k/m]$ à $\lfloor x + k/m \rfloor$ et en sommant d'abord sur k. Votre réponse s'accorde-t-elle avec (3.26) ?

18 Montrez que le terme d'erreur S de (3.30) est au plus égal à $\lceil \alpha^{-1} \nu \rceil$. *Suggestion :* montrez que les petites valeurs de j n'y contribuent pas.