LA DIVISION EN BASE b

Raymond SEROUL

Soit $b > 1$ un entier quelconque. On sait que tout entier $x > 0$ s'écrit de manière unique sous la forme :

$$x = x_n b^n + x_{n-1} b^{n-1} + \cdots + x_0 \tag{1}$$

si l'on impose les conditions

$$0 \leq x_i < b \quad \text{pour} \quad i = 0, \ldots, n \quad \text{et} \quad x_n \neq 0. \tag{2}$$

Par la suite, nous noterons $x = \overline{x_n x_{n-1} \cdots x_0}$ l'égalité (1).

Soient $x = \overline{x_n x_{n-1} \cdots x_0}$ et $y = \overline{y_p y_{p-1} \cdots y_0}$ deux entiers ($x_n \neq 0$, $y_p \neq 0$). On sait qu'il existe un unique couple (q, r) d'entiers qui satisfait

$$x = qy + r, \qquad 0 \leq r < y.$$

Nous avons tous appris, dans notre première jeunesse, un algorithme qui détermine les chiffres de q et r à partir de ceux de x et y. Comparé aux algorithmes de l'addition, de la soustraction et de la multiplication, cet algorithme est complexe et nécessite une certaine dose d'expérimentation; d'où sa mauvaise réputation. Quiconque a essayé de programmer l'algorithme de la division en base b a éprouvé de nouveau ces difficultés. Nous allons donc décrire en détail cet algorithme et le démontrer. En outre, nous verrons quels problèmes se posent lorsque l'on passe à la programmation.

1. La règle du jeu

Nous supposerons que nous ne connaissons que les tables d'addition et de multiplication en base b. En clair, cela signifie que :

- nous savons effectuer des additions, des soustractions et des multiplications en base b;
- par contre, nous ne savons pas effectuer de division. Au stade où nous en sommes, tout ce que nous nous savons faire, c'est effectuer la division d'un nombre ayant au plus deux chiffres par un nombre à un chiffre (en 'lisant à l'envers' la table de multiplication).

2. La division en base b

Commençons par nous rafraîchir la mémoire. Nous travaillons en base dix. Il s'agit de diviser $x = 1\,562\,693$ par $y = 237$.

	ξ						y			
$x \to$	1	5	6	2	6	9	3	2	3	7
$q_1 y \to$	1	4	2	2	.	.	.	6	5	9	3
$s_1 \to$		1	4	0	6	.	.	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$
$q_2 y \to$		1	1	8	5	.	.	q_1	q_2	q_3	q_4
$s_2 \to$			2	2	1	9	.				
$q_3 y \to$			2	1	3	3	.				
$s_3 \to$					8	6	3				
$q_4 y \to$					7	1	1				
$r_4 \to$					1	5	2				

Division de $x = 1\,562\,693$ *par* $y = 237$.

• On recherche d'abord le plus petit entier $\xi \geq y$ formé avec les premiers chiffres de x. On trouve $\xi = 1\,562$.

• On détermine la partie entière de ξ/y en posant la question : *en 1562, combien va-t-il de fois 237 ?* Comme nous ne connaissons que la table de multiplication, nous ne savons pas répondre à cette question. Nous supprimons alors deux chiffres à la fin des deux nombres et nous remplaçons la question précédente par la question : *en 15, combien va-t-il de fois 2 ?* La réponse $q_1 = 7$ est trop forte puisque $7 \times 237 = 1659 > 1562$. On diminue donc q_1 d'une unité; comme $6 \times 237 \leq 1562$, on sait que $q_1 = 6$ est la partie entière désirée.

• On calcule $r_1 = \xi - q_1 y = 140$, puis on abaisse le chiffre suivant de x, ce qui donne $s_1 = 1\,406$.

• On détermine la partie entière de s_1/y par le même procédé : *dans 14, combien va-t-il de fois 2 ?* La réponse $q_2 = 7$ est trop forte : $7 \times 237 = 1659 > 1406$. On diminue donc q_2 d'une unité pour constater que ce n'est pas encore la bonne réponse : $6 \times 237 = 1422 > 1406$. Il faut donc recommencer pour obtenir la bonne partie entière : $q_2 = 5$.

• On calcule $r_2 = s_1 - q_2 y = 221$, puis on abaisse le chiffre suivant de x pour obtenir $s_2 = 2\,219$.

• On détermine la partie entière de $2\,219/237$. La question : *en 22, combien va-t-il de fois 2 ?* donne une réponse trop élevée pour un chiffre. On commence donc avec $q_3 = 9$, qui est d'ailleurs la bonne réponse.

• L'algorithme se poursuit : $r_3 = s_2 - q_3 y = 86$ et $s_3 = 863$, puis $q_4 = 3$.

• La division s'achève avec $r_4 = s_3 - q_4 y = 152$.

3. Justification de l'algorithme

L'algorithme de la division euclidienne consiste donc à définir deux suites récurrentes $r_1, \ldots, r_{m+1}$ et $s_1, \ldots, s_m$:

$$\text{(3)} \qquad \begin{aligned} r_i &= s_{i-1} - q_i y, \\ s_i &= b r_i + x_{m-i}, \qquad (s_0 = \xi), \end{aligned}$$

où $\xi = \overline{x_n \cdots x_m}$ est le plus petit entier $\geq y$ formé avec les premiers chiffres de x et où $q_i = [s_{i-1}/y]$, le crochet désignant la partie entière.

$$
\begin{array}{rl|l}
 & \overbrace{x_n \cdots x_m}^{s_0}\ x_{m-1} \cdots x_0 & y \\
\hline
 & \left\{\begin{array}{l} r_1 = s_0 - q_1 y \\ s_1 = b r_1 + x_{m-1} \end{array}\right. & q_1 \cdots q_{m+1} \\
 & \left\{\begin{array}{l} r_2 = s_1 - q_2 y \\ s_2 = b r_2 + x_{m-2} \end{array}\right. & q_i = [s_{i-1}/y] \\
 & \cdots & \\
 & \left\{\begin{array}{l} r_m = s_{m-1} - q_m y \\ s_m = b r_m + x_0 \end{array}\right. & \\
 & r_{m+1} = s_m - q_{m+1} y &
\end{array}
$$

Description de la division en base b.

Théorème 1.— *L'algorithme de la division détermine correctement les chiffres du quotient.*
Quelle information pouvons-nous déduire de (3)? En multipliant par b^{m-i} l'égalité $r_i = b r_{i-1} + x_{m-i+1} - q_i y$ pour $i = m, \ldots, 0$,

$$
\begin{array}{l|l}
b^m & r_1 = \xi - q_1 y \\
b^{m-1} & r_2 = b r_1 + x_{m-1} - q_2 y \\
\cdots & \cdots \\
b & r_m = b r_{m-1} + x_1 - q_m y \\
1 & r_{m+1} = b r_m + x_0 - q_{m+1} y
\end{array}
$$

et, en ajoutant membre à membre, on obtient

$$x = (q_1 b^m + q_2 b^{m-1} + \cdots + q_{m+1}) y + r_{m+1}. \tag{4}$$

Si les q_i sont des chiffres (c'est-à-dire si $0 \leq q_i < b$) et si $0 \leq r_{m+1} < y$, nous savons que l'écriture du quotient dans la base b est $\overline{q_1 \cdots q_{m+1}}$.
Commençons par prouver que l'on a

$$y \leq \xi < by.$$

Posons $\zeta = \overline{x_n \ldots x_{m+1}}$, de sorte que $\xi = b\zeta + x_m$. Vu la définition de ξ, nous avons $\zeta < y$, ce qui s'énonce encore $\zeta \leq y - 1$. Il en résulte que $\xi \leq b(y-1) + b - 1 \leq by - 1 < by$.
La double inégalité $y \leq \xi < by$ montre que $q_1 = [\xi/y]$ est un chiffre différent de 0. Puisque $\xi = q_1 y + r_1$, nous voyons que $0 \leq r_1 < y$. De l'inégalité $s_1 = b r_1 + x_{m-1} \leq b(y-1) + b - 1 = by - 1$, on déduit aussitôt que q_2 est un chiffre. Une récurrence facile permet de conclure. □

déterminer $\xi = \overline{x_n \cdots x_m}$;
$q_1 := [\xi/y]$; $r_1 := \xi - q_1 y$;
for $i := 1$ **to** m **do begin**
  $s_i := br_i + x_{m-i}$;
  $q_{i+1} := [s_i/y]$;
  $r_{i+1} := s_i - q_{i+1} y$;
  end ;
end ;

Algorithme de la division (version idéale).

4. Estimation efficace des parties entières

Pour estimer la partie entière $[u/v]$ *(en u, combien va-t-il de fois v ?)*, nous n'avons droit qu'à la table de multiplication. C'est pour cette raison que nous remplaçons $q = [u/v]$ par une estimation $\bar{q}$ obtenue en changeant de question.
Décrivons de manière précise ce changement. Soient u et v deux entiers qui vérifient $0 < v \leq u < bv$, de sorte que $q = [u/v]$ est un chiffre différent de zéro.

- Si u et v ont le même nombre de chiffres, soit $\bar{u}$ le premier chiffre de u. Si u a un chiffre de plus que v, soit $\bar{u}$ le nombre formé des deux premiers chiffres de u.
- Soit $\bar{v}$ le premier chiffre de v.

Pour simplifier l'exposé, introduisons quelques notations :

$$u = \overline{u_{n+1} u_n \cdots u_0}, \quad v = \overline{v_n \cdots v_0}.$$

(Si u et v ont le même nombre de chiffres, on a $u_{n+1} = 0$.) Nous avons donc $\bar{u} = \overline{u_{n+1} u_n}$ et $\bar{v} = v_n$. Posons encore $B = b^n$ et

$$\bar{\bar{u}} = \overline{u_{n-1} \cdots u_0}, \quad \bar{\bar{v}} = \overline{v_{n-1} \cdots v_0},$$

de sorte que $u = B\bar{u} + \bar{\bar{u}}$ et $v = B\bar{v} + \bar{\bar{v}}$ avec $\bar{\bar{u}} < B$ et $\bar{\bar{v}} < B$.

En ne disposant que de la table de multiplication, tout ce que nous pouvons faire c'est estimer $q = [u/v]$ par le nombre

$$\bar{q} = \min\left\{b - 1, \left[\frac{\bar{u}}{\bar{v}}\right]\right\}. \tag{5}$$

Plusieurs théorèmes vont préciser la validité de cette estimation.
Théorème 2.— *On a toujours* $q \leq \bar{q}$.

Démonstration. — Si $\bar{q} = b - 1$, c'est terminé. Supposons alors $\bar{q} = [\bar{u}/\bar{v}]$. Nous pouvons écrire

$$\frac{u}{v} = \frac{B\bar{u} + \bar{\bar{u}}}{B\bar{v} + \bar{\bar{v}}} \leq \frac{B\bar{u} + b - 1}{B\bar{v}}.$$

Vu la croissance de la fonction partie entière, la démonstration sera terminée si nous prouvons que la partie entière de $(B\bar{u}+b-1)/(B\bar{v})$ est $\bar{q}$. Pour cela, il suffit d'établir les inégalités

$$\bar{q} \leq \frac{B\bar{u}+b-1}{B\bar{v}} < \bar{q}+1.$$

L'inégalité de gauche est immédiate

$$\bar{q} \leq \frac{\bar{u}}{\bar{v}} = \frac{B\bar{u}}{B\bar{v}} < \frac{B\bar{u}+b-1}{B\bar{v}}.$$

Pour prouver l'inégalité de droite, partons de $[\bar{u}/\bar{v}] < \bar{q}+1$, ce qui s'écrit encore $\bar{u} \leq (\bar{q}+1)\bar{v}-1$. A partir de là, on a

$$\begin{aligned} B\bar{u}+b-1 &\leq B\big((\bar{q}+1)\bar{v}-1\big)+b-1 \\ &\leq B(\bar{q}+1)\bar{v}-1 < B(\bar{q}+1)\bar{v} \end{aligned}$$

si $b-B \leq 0$, ce qui est vrai lorsque $n \geq 1$. Lorsque $n=0$, on a $u = \overline{u_1 u_0} = \bar{u}$, $v = v_0 = \bar{v}$ et $B=1$, ce qui entraîne

$$\bar{q} \leq \left[\frac{\bar{u}}{\bar{v}}\right] \leq \left[\frac{\bar{u}+b-1}{\bar{v}}\right]. \quad \square$$

Puisque nous savons que l'estimation $\bar{q}$ donnée par la formule (5) est une majoration, nous pouvons reformuler de manière plus réaliste l'algorithme de la division : on démarre avec $q := \bar{q}$, puis on diminue q jusqu'à ce que l'on obtienne $u - q \times v \geq 0$. Nous trouvons ainsi l'algorithme que l'on apprend aux enfants.

déterminer $\xi = \overline{x_n \cdots x_m}$;
$s_0 := \xi$;
for $i := 1$ **to** m **do begin**
  $q_i :=$ estimation(s_{i-1}, y) ;
  $r_i := s_{i-1} - q_i y$;
  rectifier(r_i, q_i)
  $s_i := b r_i + x_{m-i}$;
end ;
$q_{m+1} :=$ estimation(s_m, y) ;
$r_{m+1} := s_m - q_{m+1} y$;
rectifier(r_{m+1}, q_{m+1})

Algorithme de la division (version réaliste).

Cet algorithme utilise la fonction estimation définie par la formule (5) et la procédure rectifier :

```
procedure rectifier(var r, q) ;
begin
  | while r < 0 do begin
  |     | r := r + y ; q := q − 1
  |   end
end ;
```

La procédure rectifier.

Cependant, ce nouvel algorithme est particulièrement inefficace car l'estimation $\bar{q}$ de q est parfois catastrophique. Lorsque $x = 99$ et $y = 19$, on a $\bar{q} = 9$ et $q = 5$. Ce phénomène n'est pas particulier à la base dix.
En base b, si nous posons $\beta = b - 1$, l'exemple $x = \overline{100} = b^2$ et $y = \overline{1\beta} = 2b - 1$ montre que $\bar{q} \simeq b$ alors que $q \simeq \frac{1}{2}\, b$ si b est grand. Si nous travaillons avec une grande base b, il est donc possible que la boucle de la procédure rectifier soit sollicitée environ $\frac{1}{2}\, b$ fois!

Ce sont les tentatives de programmation de la division qui font prendre conscience de ce problème. Tant que nous travaillons en base dix, nous utilisons simultanément l'estimation (5) et notre intuition, ce qui nous permet de trouver rapidement la bonne réponse. Par exemple, pour $u = 1\,462$ et $v = 237$, nous avons $q = 6$ et $\bar{q} = 7$. Cependant, nous *sentons* que $q = 7$ est une réponse incorrecte. Aussi, nous essayons tout de suite $\bar{q} = 6$, sans passer par l'étape $\bar{q} = 7$.

Heureusement, il est possible de départager les bons cas des mauvais :
Théorème 3.— *Si le premier chiffre de v dépasse $\frac{1}{2}\, b$, alors $\bar{q} - q \leq 2$.*

Démonstration. — Nous allons démontrer la contraposée

$$\bar{q} - q \geq 3 \implies \bar{v} < \tfrac{1}{2}\, b.$$

Les inégalités $v - B = B\bar{v} + \bar{\bar{v}} - B$ et $\bar{\bar{v}} \leq B - 1$ montrent que

$$v - B < B\bar{v}.$$

Nous savons que $v \geq B$. Mais $v = B$ implique $\bar{q} = q$. Par conséquent, nous avons $v - B > 0$.
La définition de $\bar{q}$ montre que $\bar{q} \leq \bar{u}/\bar{v} \leq (B\bar{u})/(B\bar{v}) < u/(v - B)$. De manière analogue, nous avons $u/v < q+1$. En combinant ces deux inégalités, nous obtenons :

$$3 \leq \bar{q} - q < \frac{u}{v - B} - \frac{u}{v} + 1$$

ce qui s'écrit encore

$$2 < \frac{u}{v}\,\frac{B}{v - B} \leq \frac{u}{v}\,\frac{B}{B\bar{v} - B} = \frac{u}{v}\,\frac{1}{\bar{v} - 1}.$$

Sachant que $u < bv$, nous obtenons enfin

$$2 < \frac{b}{\bar{v} - 1}$$

ce qui s'écrit encore $\bar{v} \leq \frac{1}{2}(b-1)$. □

Que faire si le premier chiffre de v n'est pas assez grand? Une solution consiste à remplacer u et v par δu et δv, en espérant qu'un multiple convenable δv de v ait un premier chiffre assez grand. En procédant ainsi, on ne modifie pas le quotient. Seul le reste est multiplié par δ.

Théorème 4.— Posons $\delta = [b/(\bar{v}+1)]$. Alors δv a autant de chiffres que v et le premier chiffre de δv est plus grand que $\frac{1}{2}b$.

Démonstration. — Tout d'abord, δ n'est jamais nul puisque $\bar{v} < b$. De la définition $\delta \leq b/(\bar{v}+1) < \delta + 1$ et de $\bar{\bar{v}} < B$, on tire

$$\delta y = \delta(B\bar{v} + \bar{\bar{v}}) < \frac{bB\bar{v}}{1+\bar{v}} + \frac{bB}{1+\bar{v}} = bB,$$

ce qui prouve que δy a autant de chiffres que v. Il en résulte que le premier chiffre c_1 de δv est de la forme

$$c_1 = \delta\bar{v} + \text{retenue éventuelle provenant de } \delta\bar{\bar{v}}.$$

Cela nous permet d'écrire

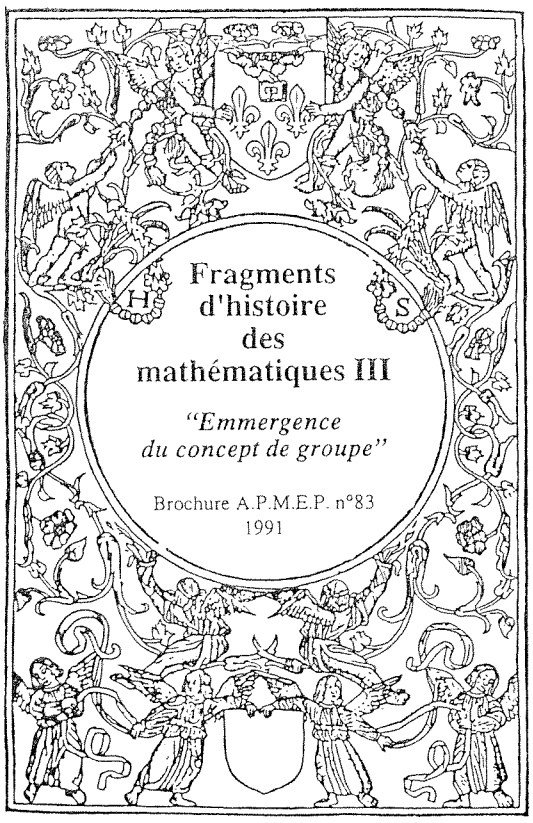
$$c_1 \geq \delta\bar{v} > \Big(\frac{b}{\bar{v}+1} - 1\Big)\bar{v} = \frac{(b-\bar{v}-1)\bar{v}}{\bar{v}+1} \geq \frac{b-2}{2}\cdot \quad \square$$

5. Le bon algorithme

Si nous prenons la précaution de *préparer* x et y (ce qui signifie remplacer x et y par δx et δy de manière que le premier chiffre de δy soir plus grand que $\frac{1}{2}b$), nous sommes sûrs que $\bar{q} = q$, $q+1$ ou $q+2$. La boucle de la procédure rectifier sera traversée au plus deux fois.

$\delta := 1$;
if $2y_p < b$ **then begin**
  $\delta := b$ **div** $(1 + y_p)$;
  $x := \delta x$; $y := \delta y$
end ;
déterminer $\xi = \overline{x_n \cdots x_m}$;
$s_0 := \xi$;
for $i := 1$ **to** m **do begin**
  $q_i := \text{estimation}(s_{i-1}, y)$;
  $r_i := s_{i-1} - q_i y$;
  $\text{rectifier}(r_i, q_i)$
  $s_i := br_i + x_{m-i}$;
end ;
$q_{m+1} := \text{estimation}(s_m, y)$;
$r_{m+1} := s_m - q_{m+1} y$;
$\text{rectifier}(r_{m+1}, q_{m+1})$;
if $\delta > 1$ **then** $r_{m+1} := x - qy$

Algorithme de la division (version définitive).



Introduction : Maurice CARMAGNOLE
Avertissement
Résumé : article paru dans l'OUVERT (Sept 86)
Emergence du Concept de Groupe

LAGRANGE : Réflexions sur la résolution algébrique des équations (1770 - 1771)

VANDERMONDE : Mémoire sur la résolution des équations (1771)

RUFFINI : Première démonstration de l'impossibilité de résoudre par radicaux l'équation générale du 5ème degré

CAUCHY : Mémoire sur le nombre de valeurs qu'une fonction peut acquérir (1815)

ABEL : Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le 4ème degré

GAUSS : Des équations qui déterminent les sections circulaires (1801)

ABEL : Mémoire sur une classe particulière d'équations résolubles algébriquement (1829)

GALOIS : Le Premier Mémoire

Chronologie
Indications pour les exercices et réponses
Bibliographie
Autres ouvrages de références