Evidences arithmétiques

Gaëtan Bayle des Courchamps

Janvier 2003
(révision 15 Août 2007)

Table des matières

1 Introduction

En se penchant sur les devoirs de classe de leurs rejetons, nombre de parents doivent s'avouer qu'ils savent les faire, sans pouvoir les expliquer autrement que par un vague "c'est évident" qui ne produit en général qu'un soupir de découragement.
En effet, qui vous prouve que $3 \times 0 = 0$, que $(-1) \times x = (-x)$, que $(-3) \times (-2) = 2 \times 3$ ou encore que $\frac{3}{4} \times \frac{5}{3} = \frac{3 \times 5}{4 \times 3}$? De même, pourquoi pose-t-on $A^{(-n)} = 1/A^n$ ou encore $A^0 = 1$?
Ce document fournit des réponses pour de nombreuses questions de ce genre que je me suis longtemps posées. Il ne saurait être fourni en guise d'explication à un écolier, mais il se veut une aide pour ceux qui auront à en formuler une.

2 Propriétés de base

2.1 Propriétés admises

Proposition 2.1 (Propriétés admises pour l'addition) *L'addition :*
- *est commutative :* $\forall(x,y), \quad x+y=y+x$
- *est associative :* $\forall(x,y,z), \quad (x+y)+z=x+(y+z)$
- *a* 0 *pour neutre :* $\forall x, \quad x+0=0+x=x$

Proposition 2.2 (Propriétés admises pour la multiplication) *La multiplication :*
- *est commutative :* $\forall(x,y), \quad x\times y=y\times x$
- *est associative :* $\forall(x,y,z), \quad (x\times y)\times z=x\times(y\times z)$
- *a* 1 *pour neutre :* $\forall x, \quad x\times 1=1\times x=x$
- *est distributive :* $\forall(x,y,z), \quad x\times(y+z)=(x\times y)+(x\times z)$ *et* $(x+y)\times z=(x\times z)+(y\times 7)$.

Remarque : La distributivité fournit une astuce pour ceux qui ont du mal à se rappeler les tables de multiplication. Par exemple $8\times 7=8\times(5+2)=(8\times 5)+(8\times 2)=40+16=56$.
Remarque : Les propriétés de distributivité, commutativité, associativité peuvent être démontrées, mais il faut partir d'axiomes nettement plus abstraits, et les démonstrations sont techniques et ennuyeuses.

3 Propriétés des nombres relatifs

Les règles de calcul usuelles sur les nombres relatifs découlent directement de la conservation des propriétés évoquées dans la section précédente: commutativité, associativité, existence d'un neutre et distributivité.

Proposition 3.1 (Opposé d'un nombre) *Pour tout nombre* x*, on admet qu'il existe au moins un autre nombre* y *tel que* $x+y=0$.
*C'est l'*opposé *de* x*. Alors :*
- *l'opposé est unique et est noté* $(-x)$
- $\forall x, \quad x=-(-x)$ *(i)*
- $\forall x, \quad 0\times x=0$ *(ii)*
- $\forall x, \quad (-1)\times x=(-x)$ *(iii)*
- $\forall(x,y), \quad x-y=x+(-y)$ *(iv)*

Preuve :
- Si y et z sont tous deux opposés à x, alors $y+x=0$ et $z+x=0$. Donc :

$$\begin{array}{rcll} y+x & = & z+x & \\ y+x+y & = & z+x+y & \text{Ajout de } y \\ y+(x+y) & = & z+(x+y) & \text{Associativité} \\ y+0 & = & z+0 & \text{Car } y \text{ est opposé à } x \\ y & = & z & \text{Car 0 est neutre pour } + \end{array}$$

- Si $x+(-x)=0$, alors, par commutativité, $(-x)+x=0$ donc $x=-(-x)$.
-
$$\begin{array}{rcll} (1+0)\times x & = & (1\times x)+(0\times x) & \text{Distributivité} \\ 1\times x & = & (1\times x)+(0\times x) & \text{Car } 1+0=1 \text{ par def. du neutre de } + \\ x & = & x+(0\times x) & \text{Car } 1\times x=x \text{ par def. du neutre de } \times \\ (-x)+x & = & (-x)+x+(0\times x) & \text{Addition de } (-x) \\ 0 & = & 0+(0\times x) & \text{Par associativité et car } (-x)+x=0 \\ 0 & = & 0\times x & \text{Car 0 est neutre pour } + \end{array}$$
-
$$\begin{array}{rcll} (1+(-1))\times x & = & 0\times x & \text{Car } 1+(-1)=0 \\ (1\times x)+((-1)\times x) & = & 0 & \text{Distributivité} \\ x+((-1)\times x) & = & 0 & \text{Car } 1\times x=x \\ (-1)\times x & = & (-x) & \text{Définition et unicité de l'opposé} \end{array}$$
-
$$\begin{array}{rcll} x-y & = & (x-y)+0 & \\ & = & (x-y)+(y+(-y)) & \\ & = & ((x-y)+y)+(-y) & \text{Associativité.} \\ & = & x+(-y) & \text{Par définition de la soustraction :} (x-y)+y=x \end{array}$$

■

Proposition 3.2 (Règles sur les signes) • $(-1) \times (-1) = 1$
- $(-x) \times (-y) = x \times y$
- $(-x) \times y = -(xy)$

Preuve : •

$$\begin{array}{rcll} (-1) \times ((-1)+1) & = & (-1) \times 0 & \text{Car } 1+(-1)=0 \\ (-1) \times ((-1)+1) & = & 0 & \text{Car } (-1) \times 0 = 0 \\ ((-1) \times (-1)) + ((-1) \times 1) & = & 0 & \text{Distributivité} \\ ((-1) \times (-1)) + (-1) & = & 0 & \text{Car } (-1) \times 1 = (-1) \\ (-1) \times (-1) & = & -(-1) & \text{Formule } x + (-x) = 0 \\ (-1) \times (-1) & = & 1 & \text{Formule } x = -(-x) \end{array}$$

•

$$\begin{array}{rcll} (-x) \times (-y) & = & ((-1) \times x) \times ((-1) \times y) & \text{Car } (-x) = (-1) \times x, \quad (-y) = (-1) \times y \\ & = & (-1) \times x \times (-1) \times y & \text{Associativité} \\ & = & (-1) \times (-1) \times x \times y & \text{Commutativité} \\ & = & ((-1) \times (-1)) \times (x \times y) & \text{Associativité} \\ & = & 1 \times (x \times y) & \text{Car } (-1) \times (-1) = 1 \\ & = & x \times y & \text{Car 1 est neutre pour } + \end{array}$$

•

$$\begin{array}{rcll} (-x) \times y & = & ((-1) \times x \times y & \text{Car } (-x) = (-1) \times x \\ & = & (-1) \times x \times (-1) \times y & \text{Associativité} \\ & = & (-1) \times x \times y & \text{Commutativité} \\ & = & (-1) \times (x \times y) & \text{Associativité} \\ & = & -(x \times y) & \text{Formule } -x = (-1) \times x \end{array}$$

■

3.1 Règles de manipulation des parenthèses

Proposition 3.3 (Suppression des parenthèses) • $a + (b - c) = a + b - c$
- $a - (b + c) = a - b - c$
- $a - (b - c) = a - b + c$

Preuve : •

$$\begin{array}{rcll} a + (b - c) & = & a + (b + ((-1) \times c)) & \text{Propriétés de l'opposé} \\ & = & a + b + ((-1) \times c) & \text{Associativité de } + \\ & = & (a + b) + ((-1) \times c) & \\ & = & (a + b) - c & \\ a + (b - c) & = & a + b - c & \text{Ordre de calcul standard} \end{array}$$

•

$$\begin{array}{rcll} a - (b + c) & = & a + ((-1) \times (b + c)) & \text{Propriétés de l'opposé} \\ & = & a + ((-1) \times b + (-1) \times c) & \text{Distributivité} \\ & = & a + ((-1) \times b) + ((-1) \times c) & \text{Associativité de } + \\ & = & a - b + ((-1) \times c) & \text{Propriétés de l'opposé} \\ & = & a - b - c & \text{Propriétés de l'opposé} \end{array}$$

•

$$\begin{array}{rcll} a - (b - c) & = & a + (-1) \times (b + (-1) \times c) & \text{Propriétés de l'opposé} \\ & = & a + (-1) \times b + (-1) \times (-1) \times c & \text{Distributivité} \\ & = & a + (-1) \times b + c & \text{Car } (-1) \times (-1) = 1 \\ & = & a - b + c & \text{Propriétés de l'opposé} \end{array}$$

■

4 Propriété des fractions

En admettant qu'une fractions $\frac{a}{b}$ est l'unique nombre tel que $\frac{a}{b} \times b = a$, on obtient les règles habituelles rien qu'en exploitant les propriétés évoquées plus haut.

Proposition 4.1 (Calculs habituels sur les fractions) • $\frac{a}{a} = 1$
- $\frac{a}{b} + \frac{c}{b} = \frac{a+c}{b}$
- $\frac{a}{b} \times \frac{c}{d} = \frac{a \times c}{b \times d}$
- $\frac{a}{b} + \frac{c}{d} = \frac{(a \times d) + (c \times b)}{b \times d}$

Preuve : •

$$\begin{array}{rcll} \frac{a}{a} \times a & = & a & \text{Par définition} \\ \frac{a}{a} & = & a \div a & \text{Définition de la division} \\ \frac{a}{a} & = & 1 & \text{Car } a \times 1 = a \end{array}$$

•

$$\begin{array}{rcll} \left(\frac{a}{b} \times \frac{c}{d}\right) \times (b \times d) & = & \left(\frac{a}{b} \times b\right) \times \left(\frac{c}{d} \times d\right) & \text{Associativité, commutativité de } \times \\ & = & a \times c & \text{Définition de } \frac{a}{b} \text{ et } \frac{c}{d} \\ \frac{a}{b} \times \frac{c}{d} & = & \frac{a \times c}{b \times d} & \text{Définition de } \frac{a \times c}{b \times d} \end{array}$$

•

$$\begin{array}{rcll} \left(\frac{a}{b} + \frac{c}{b}\right) \times b & = & \frac{a}{b} \times b + \frac{c}{b} \times b & \text{Distributivité} \\ \left(\frac{a}{b} + \frac{c}{b}\right) \times b & = & a + c & \text{Définition de } \frac{a}{b} \text{ et } \frac{c}{b} \\ \frac{a}{b} + \frac{c}{b} & = & \frac{a+c}{b} & \text{Définition de } \frac{a+c}{b} \end{array}$$

•

$$\begin{array}{rcll} \frac{a}{b} + \frac{c}{d} & = & \left(\frac{a}{b} \times \frac{d}{d}\right) + \left(\frac{c}{d} \times \frac{b}{b}\right) & \text{Car } \frac{b}{b} = \frac{d}{d} = 1 \\ & = & \frac{a \times d}{b \times d} + \frac{c \times b}{d \times b} & \text{Multiplication de fractions} \\ & = & \frac{a \times d}{b \times d} + \frac{c \times b}{b \times d} & \text{Car } b \times d = d \times b \\ & = & \frac{a \times d + c \times b}{b \times d} & \text{Somme de fractions, même dénominateur } b \times d \end{array}$$

■

5 Algèbre linéaire

L'idée de base de l'algèbre repose sur le principe de substitution : si une expression E_0 dépend d'une expression E_1, et si $E_1 = E_2$, alors on peut remplacer E_1 par E_2 dans E_0. Exemple :

$$\begin{array}{rcll} x & = & 2x - y & (E_0) \\ y & = & 3x & (E_1) = (E_2) \end{array}$$

On remplace y par $3x$ dans E_0, ce qui donne le système équivalent :

$$\begin{array}{rcll} x & = & 2x - 3x & (E_0) \\ y & = & 3x & (E_1) = (E_2) \end{array}$$

Proposition 5.1 (Combinaison de lignes) *Soit le système* $\left\{ \begin{array}{rcll} A & = & B & (i) \\ C & = & D & (ii) \end{array} \right.$
Alors :
- $A + C = B + D, \quad A \times C = D \times B, etc.$
- $\forall (\alpha, \beta), \quad \alpha A + \beta C = \alpha B + \beta D$

Preuve : •

$$\begin{array}{rcll} A & = & B & \text{Hypothèse } (i) \\ A + C & = & B + C & \text{Ajout de } C \text{ à chaque membre} \\ A + C & = & B + D & \text{Car } C = D \text{ d'après } (ii) \end{array}$$

• Le second point découle du premier: en multipliant, par α, chaque membre de (i), on obtient $\alpha A = \alpha B \quad (iii)$. De même $\beta C = \beta D \quad (iv)$.
Le premier point appliqué à (iii) et (iv) donne alors $\alpha A + \beta C = \alpha B + \beta D$. ■

Proposition 5.2 (Equivalence de systèmes) *Soit un système* $S_0 \left\{ \begin{array}{rcll} A & = & B & (E_1) \\ C & = & D & (E_2) \end{array} \right.$ *Alors pour tout nombre* α*,* S_0 *est équivalent au système :*

$$S_1 \left\{ \begin{array}{lcll} A & = & B & (E_1) \\ C + \alpha\, A & = & D + \alpha\, B & (E_3) = (E_2 + \alpha\, E_1) \end{array} \right.$$

Preuve : • ($\Longrightarrow$) Supposons S_0 vérifié. La proposition sur les combinaisons de ligne entraîne la validité de (E_3), donc $(S_0) \Rightarrow (S_1)$

• ($\Longleftarrow$)Supposons (S_1) vérifié. Appliquons la proposition sur les combinaisons de ligne dans (S_1), en faisant $(E_4) \longleftarrow (E_3) - \alpha(E_1)$. Alors $C + \alpha\, A - \alpha\, A = D + \alpha\, B - \alpha\, B$ i.e. $C = D \quad (E_2)$. On retrouve alors le système de départ, donc $(S_1) \Rightarrow (S_0)$.

• Donc par double implication $(S_0) \Longleftrightarrow (S_1)$. ∎

6 Opérations courantes

6.1 Addition de nombres entiers positifs

On commence à additionner les unités. S'il y en a 10 ou plus, on ajoute une dizaine et on enlève 10 unités. Puis on additionne les dizaines : s'il y en a plus de 10, alors on en retire 10, et on ajoute une centaine. On répète ce manège pour les centaines, les milliers, etc.

	5	9	2	5 centaines, 9 dizaines, 2 unités
+	8	3	7	8 centaines, 3 dizaines, 7 unités
			9	$2 + 7 = 9$ unités
	5	9		5 centaines, 9 dizaines
	8	3		8 centaines, 3 dizaines
			9	9 unités
	1	2		$9 + 3 = 12$ dizaines $= 1$ centaine, 2 dizaines
	5			5 centaines
	8			8 centaines
		2	9	2 dizaines, 9 unités
1	4			$1 + 5 + 8 = 14$ centaines $= 1$ millier, 4 centaines
1	4	2	9	Résultat final 1 millier, 4 centaines, 6 dizaines, 9 unités

6.2 Soustraction de nombres entiers positifs

Même idée que pour l'addition.
On commence par retirer les unités. S'il n'y en a pas assez, alors on en ajoute 10, quitte à retirer une dizaine de plus après.
Ensuite on retire les dizaines. S'il n'y en a pas assez, on en ajoute 10, quitte à retirer une centaine de plus ultérieurement.
La suite est à l'avenant pour les centaines, les milliers, etc.

	4	0	8	6	On a un panier de 4086 bonbons.
−		8	9	1	On veut retirer 8 centaines , 9 dizaines , 1 unité.
				5	Il reste $6-1=5$ unités
	4	0	8		et 4 milliers, 0 centaine, 8 dizaines
−		8	9		Il faut encore retirer 8 centaines et 9 dizaines
				5	
	1	0	18		Pas assez de dizaines : on en ajoute 10 (= 1 centaine)
−		9	9		Il faudra donc retirer $8+1=9$ centaines
			9	5	Il reste $18-9=9$ dizaines, 5 unités
	4	0			et 4 milliers, 0 centaine
−		9			Il faut encore retirer 9 centaines.
			9	5	
	4	10			Pas assez de centaines : on en ajoute 10 (= 1 millier)
−	1	9			Il faudra donc retirer $0+1=1$ millier.
		1	9	5	Il reste $10-9=1$ centaine, 9 dizaines, 5unités.
	4				et 4 milliers
−	1				Il faut encore retirer 1 millier
	3	1	9	5	Il reste $4-1=3$ milliers, 1 centaine, 9 dizaine, 5 unités

6.3 Multiplication

6.3.1 Qu'est-ce qu'une multiplication ?

Un berger qui a disposé ses moutons en 4 lignes de 8 moutons peut les compter d'au moins deux façons :
- Additionner les colonnes : $4+4+4+4+4+4+4+4=4\times 8=32$
- Additionner les lignes : $8+8+8+8=8\times 4=32$

La multiplication évite donc, en particulier, les additions répétitives. On remarque aussi $4\times 8=8\times 4$. Cette propriété, valable pour n'importe quel nombre, est appelée *commutativité*.
Le berger aurait pu disposer ses moutons différemment. Par exemple, en séparant les colonnes : comme $5+3=8$, on peut former deux groupes de 4 lignes, le premier avec 5 colonnes, le second avec 3 colonnes. Alors le nombre des moutons est :
- En comptant dans chaque groupe $(4\times 3)+(4\times 5)=12+20=32$

En particulier, $4\times(5+3)=(4\times 5)+(4\times 3)$. c'est appelé *distributivité* ...
Associativité : $4\times 100=4\times(10\times 10)=(4\times 10)\times 10$.

6.3.2 A 1 chiffre

Imaginons que nous avons 282 rangées de 9 soldats de plomb, et que nous voulons compter le nombre total de soldats.

	2	8	2	282 rangs
×			9	de 9 soldats de plomb
		1	8	2 rangs de 9 soldats : 9×2 unités = 18 unités
	7	2		80 rangs de 9 soldats : 9×8 dizaines = 72 dizaines
1	8			200 rangs de 9 soldats : 9×2 centaines = 18 centaines
2	5	3	8	Total : $18+720+1800=2538$ unités

Avec de l'habitude, on n'écrit plus les lignes intermédiaires.

6.3.3 Intermède: multiplier par dizaines, centaines

Avant de multiplier par des nombres compliqués, tâchons de le faire proprement dans des cas simples.
Par 10 : les unités deviennent des dizaines, toutes les dizaines des centaines, etc. ce qui revient à décaler d'un chiffre vers la gauche.
Par 100 : vous vous rappelez de l'associativité ? Elle sert ici : $12,3\times 100=12,3\times(10\times 10)=(12,3\times 10)\times 10=123\times 10=1230$.
Donc multiplier par 100 revient à décaler deux fois les chiffres vers la gauche.

De même, pour multiplier par 1000, 10000, etc. il faut décaler les chiffres respectivement de 3, 4, etc. rangs vers la gauche.

6.3.4 Avec plusieurs chiffres

Qui sait effectuer des multiplications à 1 seul chiffre en une ligne, est prêt pour la multiplication à plusieurs chiffres.
Comptons les d'arbres disposés en 196 rangées de 128 dans une exploitation forestière.

		1	2	8	de 128 arbres dans chaque rangée.
	×	1	9	6	196 rangées
		7	6	8	6 rangées de 128 arbres : $6 \times 128 = 768$
1	1	7	2		9 dizaines de rangées de 128 arbres : $9 \times 128 = 1172$ dizaines
1	2	8			1 centaine de rangées de 128 arbres : $1 \times 128 = 128$ centaines
2	5	2	8	8	Total :$768 + 11720 + 12800 = 15288$ arbres

6.4 Division

Nous devons répartir 11437 billes entre 27 personnes. Remarquons d'abord que cela fait 11 milliers de billes. Or $11 < 27$ donc impossible de commencer une distribution par milliers. Par contre cela fait 114 centaines de billes. Or $114 > 27$ donc on peut distribuer par paquets de 100.

1	1	4	3	7			27		11437 billes à répartir entre 27 personnes.
−1	0	8				4	×27 =	108	4 centaines de billes par personne :108 centaines
		6	3						Restent 6 centaines et 3 dizaines = 63 dizaines de billes.
	−	5	4			2	×27 =	54	2 dizaines de billes par personne : 54 dizaines
			9	7					Restent 9 dizaines et 7 = 97 billes.
		−	8	1		3	×27 =	81	3 billes par personne :81 billes
			1	6					Restent 16 billes.
						423			Chacun reçoit 4 centaines, 2 dizaines et 3 billes, i.e. 423

7 Les puissances

Définition 7.1 (Puissances positives) *Soit a un nombre quelconque. Par récurrence, on définit A^n pour tout $n \in \mathbf{N}^*$:*
- $A^1 = A$
- $A^{n+1} = A\,A^n$

Proposition 7.2 (Exposants nuls et négatifs) *Pour tout nombre A, pour tout $(m, n) \in \mathbf{Z} \times \mathbf{Z}$:*
- $A^m A^n = A^{m+n}$
- $(A^m)^n = A^{mn}$

De plus, ces propriétés imposent :
- $A^0 = 1$
- $A^{(-n)} = \frac{1}{A^n}$

Preuve : • Posons $H_n : \forall A, \forall m \in \mathbf{N}, A^m A^n = A^{m+n}$. Si $n = 1$ alors $A^m A^n = A^m A = A^{m+1} = A^{m+n}$. Si $n >= 1$ et si H_n est vraie alors :

$$\begin{array}{rcll} A^m A^{n+1} & = & A^m A^n A^1 & \text{Définition de } A_{n+1} \\ & = & (A^m A^1) A^n & \text{Commutativité et associativité} \\ & = & A^{m+1} A^n & \text{Définition de } A_{m+1} \\ & = & A^{(m+1)+n} & \text{D'après } H_n \\ & = & A^{m+(n+1)} & \text{Associativité} \end{array}$$

donc H_{n+1} est vraie, et par récurrence H_n est vraie pour $n \geq 1$. • Posons $H_n : \forall A, \forall m \in \mathbf{N}, (A^m)^n = A^{mn}$. Si $n = 1$ alors $(A^m)^1 = A^m = A^{m\times 1} = A^m n$ donc H_1 est vraie. Si $n \geq 1$ et si H_n est vraie alors :

$$\begin{array}{rcll} (A^m)^{n+1} & = & ((A^m)^n) \times A^m & \text{Définition de l'exposant } (n+1 \\ & = & A^{mn} \times A^m & \text{D'après } H_n \\ & = & A^{mn+m} & \text{Formule précédente} \\ & = & A^{m(n+1)} & \text{Car } mn + m = m(n+1) \end{array}$$

donc H_{n+1} est vraie et par récurrence H_n est vraie pour tout $n \geq 1$. • On souhaite avant tout garder la formule $A^{m+n} = A^m \times A^n$. Ainsi, $A^1 \times A^0 = A^{1+0} = A^1$, donc $A^0 = \frac{A^1}{A^1} = 1$

• De même, $A^{-n} \times A^n = A^{(-n)+n} = A^0 = 1$, d'où $A^{(-n)} = \frac{1}{A^n}$ ∎

8 Critères de divisibilité, preuve par 9

On sait que, pour qu'un nombre (écrit en base 10) soit multiple de 3, il faut et il suffit que la somme de ses chiffres le soit; de même pour les multiples de 9; Pour 11, ça se complique alors que pour 2, 4 ou 5 il suffit de tenir en compte les derniers chiffres.
Les congruences sont un outil rêvé pour éclaircir ces distinctions. Elles prouvent de surcroît que la fameuse preuve par 9 s'applique aussi bien à l'addition qu'à la multiplication.

Définition 8.1 (Congruence modulo N) *Soit un entier N. Soient a et b deux autres entiers. Alors a est dit congru à b modulo N si et seulement si $a - b$ est multiple de N. En d'autres termes :*

$$\forall N \in \mathbf{Z}, \quad \forall (a,b) \in \mathbf{Z} \times \mathbf{Z}, \quad (a \equiv b \quad [N]) \Longleftrightarrow (\exists k \in \mathbf{Z}, \quad a = b + kN)$$

Théorème 8.2 (Congruences et opérations) *Soit $N \in \mathbf{N}^*$. On montre alors :*
• *a est multiple de N ssi $a \equiv 0 \quad [N]$*
• *Si $a \equiv b \quad [N]$ et $b \equiv c \quad [N]$ alors $a \equiv c \quad [N]$*
De plus, si $a \equiv a' \quad [N]$ et $b \equiv b' \quad [N]$ alors :
• *$a + b \equiv a' + b' \quad [N]$*
• *$a\,b \equiv a'\,b' \quad [N]$*
Enfin, si r est le reste de la division de a par N, alors :
• *$a \equiv r \quad [N]$*

Preuve : c • Par définition $a \equiv 0 \quad [N]$ signifie $\exists k \in \mathbf{Z}, \quad a = 0 + k\,N$, i.e. a est multiple de N.
• Il existe $(k,m) \in \mathbf{Z}\times\mathbf{Z}$ tels que $a = b + k\,N$ et $b = c + m\,N$. Alors : $a = c + m\,N + k\,N = c + (m+k)N$ donc $a \equiv c \quad [N]$.
• Il existe $(k,m) \in \mathbf{Z} \times \mathbf{Z}$ tels que $a = a' + k\,N$ et $b = b' + m\,N$. Alors :

$$\begin{array}{rcll} a + b & = & (a' + k\,N) + (b' + m\,N) & \text{par hypothèse} \\ a + b & = & (a' + b') + (k + m)N & \text{commutativité, associativité} \end{array}$$

• Même raisonnement dans le cas du produit :

$$\begin{array}{rcll} a\,b & = & (a' + k\,N)(b' + m\,N) & \text{par hypothèse} \\ a\,b & = & a'b' + N(b'k + a'm + kmN) & \text{commutativité, associativité} \end{array}$$

• Soit r le reste de la division euclidienne de a par N, et q son quotient. Alors $a = r + q\,N$, donc par définition $a \equiv r \quad [N]$. ∎
Remarque : Le premier point nous a montré que, pour vérifier si un nombre est multiple de N, il suffit de calculer sa valeur modulo N. Ce calcul est facilité par les points qui ont suivi.

Théorème 8.3 (Critère général de divisibilité) *Soit un nombre n écrit dans une base b avec K chiffres $a_0, \ldots, a_{K-1}$.*
Prenons, pour tout $i \in \mathbf{N}$, un nombre r_i tel que $r_i \equiv b^i [N]$. Alors n est multiple de N ssi $S = \sum_{i=0}^{K-1} r_i\,a_i$ l'est.

Preuve : Partons de la définition de l'écriture en base b, et appliquons les règles montrées dans le théorème précédent.

$$\begin{array}{rcll} n & = & \sum_{i=0}^{K-1} b^i\, a_i & \text{Ecriture de } n \text{ en base } b \\ & \equiv & \sum_{i=0}^{K-1} b^i\, a_i \quad [N] & \text{Car } n \equiv n \quad [N] \\ & \equiv & \sum_{i=0}^{K-1} r_i\, a_i \quad [N] & \text{Car } r_i \equiv b^i \quad [N] \\ n & \equiv & S \quad [N] & \text{Définition de } S \end{array}$$

Or n est multiple de N ssi $n \equiv 0 \quad [N]$, i.e. $S \equiv 0 \quad [N]$, i.e. ssi S est multiplede N ∎

Théorème 8.4 (Critères de divisibilité usuels) *Le nombre n est multiple ...*

- *de* 2 *ssi son dernier chiffre est pair*
- *de* 4 *ssi ses deux derniers chiffres forment un multiple de* 4
- *de* 3 *ssi la somme de ses chiffres est multiple de* 3
- *de* 9 *ssi la somme de ses chiffres est multiple de* 9
- *de* 5 *ssi le dernier chiffre est* 0 *ou* 5
- *de* 10 *ssi le dernier chiffre est* 0
- *de* 11 *ssi la différences entre la somme des chiffres de rang pair et celle des chiffres de rang impair forme un multiple de* 11

Preuve : Il suffit d'appliquer le theorème précédent avec une base $b = 10$, en fonction des diverses valeurs de N.

- Si $N = 2$, alors $10^0 \equiv 1 \quad [N]$ et pour tout $i \geq 1$, $10^i \equiv 0 \quad [N]$. On prend donc $r_i = 1$ si $i = 0$, $r_i = 0$ sinon.
- Si $N = 4$, comme $10 \equiv 2 \quad [4]$ on peut prendre $r_0 = 1$, $r_1 = 10$, et $r_i = 0$ pour $i \geq 2$.
- Si $N = 5$, comme $10^1 \equiv 0 \quad [5]$, on peut prendre $r_0 = 1$, et $r_i = 0$ pour $i \geq 1$
- Si $N = 3$, comme $10 \equiv 1 \quad [3]$, on peut prendre $r_i = 1$ pour tout i.
- Si $N = 11$, comme $10 \equiv (-1) \quad [11]$, on peut prendre $r_i = (-1)^i$

∎

Remarque : Pour $N = 7$, c'est malheureusement moins simple, sauf à prendre $r_0 = 1$, $r_1 = 3$, $r_2 = 2$, $r_3 = 6$, $r_4 = 4$, $r_5 = 5$ etc.

Théorème 8.5 (Divisibilité par un nombre composé) *Si a et b sont deux diviseurs de N, avec $a \wedge b = 1$, alors ab est un diviseur de N*

Preuve : Il existe k et m tels que $ak = bm = n$. Donc b divise ak. Or $a \wedge b = 1$ donc k est multiple de b. Donc $n = ak$ est multiple de ab. ∎

Théorème 8.6 (Divisibilité par 6, 12, 15, 30, 60)

- $n \equiv 0 \quad [6]$ *ssi n est multiple de* 2 *et de* 3
- $n \equiv 0 \quad [12]$ *ssi n est multiple de* 3 *et de* 4
- $n \equiv 0 \quad [15]$ *ssi n est multiple de* 3 *et* 5
- $n \equiv 0 \quad [30]$ *ssi n est multiple de* 3 *et de* 10
- $n \equiv 0 \quad [60]$ *ssi n est multiple de* 3, 4, *et* 5

Preuve :

- comme $2 \wedge 3 = 1$, on applique le théorème précédent pour $2 \times 3 = 6$
- idem avec $3 \times 4 = 12$
- idem avec $3 \times 5 = 15$
- idem avec $3 \times 10 = 30$
- idem avec $3 \times 4 \times 5 = 60$

∎

Lemme 8.7 (Somme des chiffres d'un entier) *Soit a un nombre dont les chiffres en base b s'écrivent $a_0, \ldots a_{K-1}$. Soit $S = \sum_{i=0}^{K-1} a_i$ la somme de ses chiffres. Alors $a \equiv S \quad [b-1]$.*

Preuve :

$$\begin{array}{rcll} a & = & \sum_{i=0}^{K-1} b^i\, a_i & \text{Ecriture en base } b \\ a & \equiv & \sum_{i=0}^{K-1} b^i\, a_i \quad [b-1] & \text{Car } a \equiv a \quad [b-1] \\ & \equiv & \sum_{i=0}^{K-1} 1^i\, a_i \quad [b-1] & \text{Car } b \equiv 1 \quad [b-1] \\ & \equiv & \sum_{i=0}^{K-1} a_i \quad [b-1] & \text{Car } 1^i = 1 \\ a & \equiv & S & \text{Définition de } S \end{array}$$

∎

Lemme 8.8 (Somme des chiffres, itérées) *Notons $S(\alpha)$ la somme des chiffres d'un nombre α quelconque. Soit un nombre $a > 0$. Posons $x_0 = S(a)$ et, pour tout $n \geq 0$, $x_{n+1} = S(x_n)$.*
Alors pour tout $n \in \mathbf{N}$, $x_n \equiv a \quad [b-1]$. De plus, (x_n) décroît strictement jusqu'à atteindre un seul chiffre > 0 et est stationnaire à partir de là.

Preuve : Le fait que $x_n \equiv a \quad [b-1]$ découle directement du lemme précédent. Reste la décroissance. Montrons d'abord que l'on arrive en-dessous de trois chiffres: un nombre de K chiffres est $\geq b^{K-1}$, et leur somme est $\leq (b-1)K$. Il suffit donc de montrer $P(K) : \quad (b-1)K < b^(K-1)$.
• $K = 3$: une étude élémentaire montre $2(b-1) < b^2$ pour $b \geq 2$. En effet $b^2-2(b-1) = (b^2-2b+1)+1 = (b-1)^2 + 1 > 0$
• $K >= 3$: $b^K = b.b^{K-1} > b.(b-1)K = (b-1)Kb$. Or $b \geq 2$ donc $Kb > (K+1)$ donc $b^K > (b-1)(K+1)$ donc $P(K+1)$ est vraie.
Donc (x_n) décroît et atteint $K \leq 2$ chiffres.
Si x_n est un nombre à $K = 2$ chiffres, alors leur somme est $\leq 2(b-1) = b + (b-2)$ donc, *dans la base considérée*, x_{n+1} s'écrit avec moins de 1 'dizaine' et $(b-2)$ unités. La somme des chiffres de x_{n+1} est donc $\leq 1 + (b-2) = (b-1)$. Donc x_{n+2} n'a qu'un seul chiffre!
Le nombre $x_0 = a > 0$ comporte au moins un chiffre > 0, donc $x_1 > 0$.
par récurrence, pour tout $n \in \mathbf{N}$, $x_n > 0$ ∎

Théorème 8.9 (Preuve par 9) *Prenons deux nombres a et b non-nuls, et posons $p = a\,b$. En base $b \geq 2$ fixée, itérons la somme des chiffres de a jusqu'à obtenir un nombre α à un chiffre. De même avec b, pour obtenir β. De même avec p, pour obtenir γ. De même pour $d = \alpha\beta$, pour obtenir δ.*
Alors $\delta = \gamma$.

Preuve :

$$\begin{array}{rcll} \delta & \equiv & \alpha\,\beta & [b-1] \quad \text{Lemme précédent appliqué à: } d = \alpha\beta \\ & \equiv & a\,b & [b-1] \quad \text{Car } a \equiv \alpha \quad [b-1] \text{ et } b \equiv \beta \quad [b-1] \\ & \equiv & p & [b-1] \quad \text{Définition de } p \\ \delta & \equiv & \gamma & [b-1] \quad \text{Lemme précédent appliqué à } p \end{array}$$

Le lemme précédent montre aussi $\delta > 0$ et $\gamma > 0$. Comme ces nombres n'ont qu'un chiffre en base b, on a les encadrement $1 \leq \delta \leq b-1$ et $1 \leq \gamma \leq b-1$. Donc $|\delta - \gamma| \leq b-2$. Or $\delta - \gamma$ est multiple de $b-1$, donc $\delta - \gamma = 0$ est la seule solution. D'ù $\delta = \gamma$. CQFD. ∎
Remarque : La "preuve par 9" enseignée dans les écoles consiste tout simplement à calculer α, β, γ, δ par la méthode du lemme précédent, en base $b = 10$. Le théorème est alors vérifié ... sinon c'est qu'on s'est trompé dans les calculs.
Par contre, le seul fait d'avoir $\delta = \gamma$ ne garantit nullement l'exactitude de p !
D'autre part, les congruences sont compatibles avec l'addition, donc cette 'preuve' marche aussi pour l'addition : il suffit de calculer $d = \alpha + \gamma$ au lieu de $\alpha\gamma$.

9 Extraction de racines carrées

Hum, là je doute que beaucoup de monde sache le faire. Le principe de base est cependant fort simple : il suffit encore d'appliquer la distributivité de la multiplication sur l'addition.
Personne en effet ne contestera que $(10u + v)^2 = 100u^2 + (2 \times u \times 10 + v)v$.

Proposition 9.1 (Algorithme de la racine carrée) *Soit A le nombre entier dont nous voulons extraire la racine carrée.*
• *Groupons par 2 les chiffres de A. Cela donne N nombres $a_0, \ldots, a_{N-1}$ compris entre 0 et $10^2 - 1$:*
• *En posant $b_0 = a_0$ et $b_{n+1} = 10^2 b_n + a_{n+1}$ on a $A = b_{N-1}$*
• *Définissons u_n comme le plus grand entier tel que $u_n^2 \leq b_n$.*
• *Posons alors $r_n = b_n - u_n^2$.*
Comme $A = b_{N-1}$ le problème se ramène à la recherche de u_{N-1}.
On montre que pour tout n tel que $0 \leq n < N-1$, il existe v_{n+1} tel que :
• $u_{n+1} = 10u_n + v_{n+1}$
• $0 \leq v_{n+1} < 10$
• *v_{n+1} est le plus grand nombre x tel que $100r_n + a_{n+1} \geq (2 \times u_n \times 10 + x)x$* • *Alors $r_{n+1} = (10^2 r_n + a_{n+1}) - (2 \times u_n \times 10 + v_{n+1})v_{n+1}$*

Preuve : • $b_{n+1} \geq 10^2 b_n$ donc $u_{n+1} \geq 10u_n$ donc il existe $v_{n+1} \geq 0$ tel que $u_{n+1} = 10u_n + v_{n+1}$
• Comme $a_{n+1} < 10^2$, $10^2 b_n + a_{n+1} < 10^2(b_n + 1)$. Or la condition $u_{n+1}^2 \leq b_{n+1}$ se traduit par $(10u_n + v_{n+1})^2 \leq 10^2 b_n + a_{n+1}$ donc

$$(10u_n + v_{n+1})^2 < 10^2(b_n + 1) \quad (*)$$

Supposons $v_{n+1} \geq 10$. Alors $10u_n + v_{n+1} \geq 10(u_n + 1)$ donc

$$\begin{array}{rcll} (10u_n + v_{n+1})^2 & \geq & (10(u_n+1))^2 & \\ 10^2(b_n+1) & \geq & (10(u_n+1))^2 & \text{d'après } (*) \\ b_n + 1 & \geq & (u_n+1)^2 & \\ b_n & \geq & (u_n+1)^2 & \end{array}$$

Contradiction : u_n était par définition le plus grand nombre de carré inférieur à b_n.
Donc $v_{n+1} < 10$.
• Comme $u_{n+1} = 10u_n + v_{n+1}$, v_{n+1} est le plus grand x tel que $b_{n+1} - (10u_n + x)^2 \geq 0$.

$$\begin{array}{rcl} b_{n+1} - (10u_n + x)^2 & = & 10^2 b_n + a_{n+1} - (10u_n + x)^2 \\ & = & 10^2 b_n + a_{n+1} - (10^2 u_n^2 + 20u_n x + x^2) \\ & = & 10^2(b_n - u_n^2) + a_{n+1} - (20u_n x + x^2) \\ b_{n+1} - (10u_n + x)^2 & = & (10^2 r_n + a_{n+1})) - ((2 \times u_n \times 10) + x)x \end{array}$$

Donc le plus grand x tel que $(10^2 r_n + a_{n+1})) - ((2 \times u_n \times 10) + x)x \geq 0$ est v_{n+1}.
Cette condition revient à $((2 \times u_n \times 10) + x)x \leq 10^2 r_n + a_{n+1}$
Alors

$$\begin{array}{rcll} r_{n+1} & = & b_{n+1} - u_{n+1}^2 & \\ & = & b_{n+1} - (10u_n + x)^2 & \text{pour } x = v_{n+1} \\ & = & (10^2 r_n + a_{n+1})) - ((2 \times u_n \times 10) + x)x & \text{pour } x = v_{n+1} \\ & = & (10^2 r_n + a_{n+1}) - (2 \times u_n \times 10 + v_{n+1})v_{n+1} & \end{array}$$

Et voilà! ∎

Exemple : Trouvons la racine carrée de $A = 193457$.
Groupons les chiffres par 2 : $a_0 = 19$, $a_1 = 34$, $a_2 = 57$.
A présent on peut présenter la calcul sous sa forme classique :

19	34	57	u_n	
-16			4	$b_0 = a_0 = 19$ donc $u_0 = 4$
3				$r_0 = 3$
3	34			$10^2 r_0 + a_1 = 334$
-2	49			Pour $x = 3$ on a $(2u_0 \times 10 + x) \times x = 249 \leq 334$
	85		43	donc $u_1 = 4 \times 10 + 3 = 43$ et $r_1 = 334 - (2u_0 \times 10 + 3) \times 3 = 85$
	85	57		$10^2 r_1 + a_2 = 8557$
$-$	78	21		Pour $x = 9$ on a $(2u_0 \times 10 + x) \times x = 7821 \leq 8557$
	7	36	439	donc $u_2 = 43 \times 10 + 9 = 439$ et $r_2 = 8557 - (2u_1 \times 10 + 9) \times 9 = 736$