Arithmétique 2

Alexey Muranov

17 avril 2025

Table des matières

II. Nombres entiers relatifs

II.1. Qu'est-ce que c'est, un nombre entier relatif ?

Rappelons nous que l'opération de soustraction de nombres naturels peut être appliquée à deux nombres naturels a et b à la condition que $b \leqslant a$, et que dans ce cas le résultat de cette opération est la *différence* entre a et b, notée « $a - b$ ». La valeur de la différence « $a - b$ » n'est définie comme un nombre naturel que si $b \leqslant a$.

Exercice. Essayer de compléter les tableaux suivants :

3	5	1	4	7	4
8	10	10	13	16	13
100	?	?	100	100	?

La différence entre deux nombres exprime un certain rapport entre ces nombres, qu'on pourrait appeler leur « rapport additif ». Par exemple, le « rapport additif » entre 5 et 3 est le même qu'entre 10 et 8, et le même qu'entre 102 et 100, mais différent de celui entre 7 et 4. En effet :

$$5 - 3 = 10 - 8 = 102 - 100 = 2 \neq 3 = 7 - 4.$$

Cependant, il paraît clair que le « rapport additif » entre 3 et 5 doit être le même qu'entre 8 et 10. Or, aucun nombre naturel n'exprime, dans le sens précédent, le « rapport additif » entre 3 et 5, ni entre 8 et 10, car les valeurs des différences « $3-5$ » et « $8-10$ » ne sont pas définies comme nombres naturels.

Avant de tenter de régler cette situation embarrassante, essayons de clarifier l'idée du « rapport additif ».

Notons $(\underset{+}{\simeq})$ la relation entre couples de nombres naturels dont le sens sera le suivant :

> « $(a, b) \underset{+}{\simeq} (c, d)$ » veut dire que le « rapport additif » entre b et a est le même qu'entre d et c.

Essayons de donner une définition précise de la relation $(\underset{+}{\simeq})$ en accord avec l'idée intuitive du « rapport additif ». On souhaite, en particulier, que

$$(3, 5) \underset{+}{\simeq} (8, 10) \underset{+}{\simeq} (100, 102) \underset{+}{\not\simeq} (4, 7),$$

mais aussi que

$$(5, 3) \underset{+}{\simeq} (10, 8) \underset{+}{\simeq} (102, 100) \underset{+}{\not\simeq} (3, 5).$$

Dans le cas où $a \leqslant b$ et $c \leqslant d$, on souhaite que l'équivalence suivante soit satisfaite :

$$(a, b) \underset{+}{\simeq} (c, d) \quad \Leftrightarrow \quad b - a = d - c.$$

Cependant, l'équation « $b - a = d - c$ » ne peut servir comme la définition du sens de « $(a, b) \underset{+}{\simeq} (c, d)$ » que si $a \leqslant b$ et $c \leqslant d$, car sinon, les valeurs des différences « $b - a$ » et « $d - c$ » ne sont pas toutes les deux définies (comme nombres naturels). Le problème est dans l'opération de soustraction.

Comment peut-on vérifier si $b - a = d - c$ sans utiliser l'opération de soustraction ? Une solution est évidente : il suffit de vérifier si $b + c = d + a$, car

$$b - a = d - c \quad \Leftrightarrow \quad b + c = d + a$$

dans le cas où $a \leqslant b$ et $c \leqslant d$.

Les valeurs des deux membres de l'équation « $b + c = d + a$ » (de ses parties gauche et droite) sont définies pour tous nombres naturels a, b, c, d. On va utiliser cette équation pour définir la relation $(\underset{+}{\simeq})$, qui est censée traduire l'idée intuitive du « rapport additif ».

Définition. Définissons la relation $(\underset{+}{\simeq})$ par l'équivalence suivante :

$$(a, b) \underset{+}{\simeq} (c, d) \quad \Leftrightarrow \quad b + c = d + a,$$

où a, b, c, d sont quatre nombres naturels arbitraires.

Notons que, d'après cette définition,

$$(a, b) \underset{+}{\simeq} (c, d) \quad \Leftrightarrow \quad (b, a) \underset{+}{\simeq} (d, c) \quad \Leftrightarrow \quad (a, c) \underset{+}{\simeq} (b, d) \quad \Leftrightarrow \quad (c, a) \underset{+}{\simeq} (d, b).$$

Exercice. Vérifier sur des exemples si la définition donnée ci-dessus de la relation $(\underset{+}{\simeq})$ est en accord avec l'idée intuitive du « rapport additif ».

Exercice. Soient a, b, c, d quatre nombres naturels. Montrer que $(a, b) \underset{+}{\simeq} (c, d)$ si et seulement si il existe deux nombres naturels e et f tels que $e + a = f + c$ et $e + b = f + d$.

Exercice. Trouver des nombres naturels a, b, c, d tels que

$$(5, 8) \underset{+}{\simeq} (a, 11), \qquad (5, 8) \underset{+}{\simeq} (11, b), \qquad (8, 5) \underset{+}{\simeq} (c, 11), \qquad (8, 5) \underset{+}{\simeq} (11, d),$$

s'ils existent. Combien des choix y a-t-il pour les valeurs de a, de b, de c et de d ?

Exercice. Trouver des nombres naturels a, b, c, d tels que

$$(5,8) \mathrel{\underset{+}{=}} (a,2), \qquad (5,8) \mathrel{\underset{+}{=}} (2,b), \qquad (8,5) \mathrel{\underset{+}{=}} (c,2), \qquad (8,5) \mathrel{\underset{+}{=}} (2,d),$$

s'ils existent. Combien des choix y a-t-il pour les valeurs de a, de b, de c et de d ?

Les trois propriétés suivantes de la relation $(\mathrel{\underset{+}{=}})$ sont d'une importance particulière pour la définition des entiers relatifs :

(1) si $(a,b) \mathrel{\underset{+}{=}} (c,d)$ et $(c,d) \mathrel{\underset{+}{=}} (e,f)$, alors $(a,b) \mathrel{\underset{+}{=}} (e,f)$,

(2) $(a,b) \mathrel{\underset{+}{=}} (a,b)$,

(3) si $(a,b) \mathrel{\underset{+}{=}} (c,d)$, alors $(c,d) \mathrel{\underset{+}{=}} (a,b)$.

Exercice. Démontrer ces propriétés.

Prenons en plus note des deux lemmes suivants.

Lemme. *Pour tous nombres naturels a, b, c, $(a,b) \mathrel{\underset{+}{=}} (a+c,\ b+c)$.*

Lemme. (1) *Si a, b, c sont trois nombres naturels tels que $(a,b) \mathrel{\underset{+}{=}} (a,c)$, alors $b = c$.*

(2) *Si a, b, c sont trois nombres naturels tels que $(a,c) \mathrel{\underset{+}{=}} (b,c)$, alors $a = b$.*

Exercice. Prouver ces lemmes.

Ainsi on a défini le sens de la phrase « le rapport additif entre b et a est le même qu'entre d et c » : cela veut dire que $b + c = d + a$. En plus, si $a \leqslant b$ et $c \leqslant d$, les « rapports additifs » entre b et a et entre d et c sont exprimés par les nombres naturels $b-a$ et $d-c$, et pour voir si les deux « rapports additifs » sont les mêmes, il suffit de voir si $b - a = d - c$. Mais, comme déjà mentionné, aucun nombre naturel n'exprime, dans ce sens, le « rapport additif » entre 3 et 5, ni entre 8 et 10, car les valeurs des différences « $3 - 5$ » et « $8 - 10$ » ne sont pas définies comme nombres naturels.

Une issue de cette situation est d'inventer de nouveaux nombres pour exprimer les différences entre n'importe quels nombres naturels.

Définition. Définissons les nombres *entiers*, aussi dits *entiers relatifs*, ainsi :

(1) tout nombre naturel est *entier* ;

(2) si a et b sont deux nombres naturels tels que la valeur de la différence « $b - a$ » n'est pas définie comme un nombre naturel (car $a > b$), on admet que la différence $b - a$ est un *entier* ;

(3) si a, b, c, d sont quatre nombres naturels, on admet que l'*entier* $d - c$ est le même que l'*entier* $b - a$ si et seulement si $(c,d) \mathrel{\underset{+}{=}} (a,b)$:

$$d - c = b - a \quad \Leftrightarrow \quad (c,d) \mathrel{\underset{+}{=}} (a,b) \quad \Leftrightarrow \quad b + c = d + a \ ;$$

(4) tout *entier* est la différence de deux nombres naturels.

Notation. L'ensemble des entiers relatifs sera noté « $\mathbf{Z}$ ».

Notons qu'on n'a pas besoin d'un nouveau système de numération pour écrire les nombres entiers relatifs car tout entier relatif peut être écrit comme la différence de deux nombres naturels. En plus, tout entier relatif qui n'est pas nombre naturel peut être écrit sous la forme « $0 - a$ », où a est un nombre naturel.

Notation. On adopte une écriture abrégée pour les différences de la forme « $0 - a$ » : on n'écrira pas le premier « 0 ». Ainsi, au lieu de « $0 - a$ », on peut écrire « $-a$ » tout court.

Exemple. L'expression « -42 » veut dire $0 - 42$.

II.2. Relations d'ordre usuelles

Définition. Définissons les relations $(\leqslant)$, $(\geqslant)$, $(<)$, $(>)$ entre des entiers par les équivalences suivantes, où a, b, c sont des nombres naturels arbitraires :

$$\begin{aligned} b - a \leqslant c - a \quad &\Leftrightarrow \quad b \leqslant c, & \qquad b - a \geqslant c - a \quad &\Leftrightarrow \quad b \geqslant c, \\ b - a < c - a \quad &\Leftrightarrow \quad b < c, & \qquad b - a > c - a \quad &\Leftrightarrow \quad b > c. \end{aligned}$$

Il reste à vérifier que ces définitions sont toutes correctes et complètes.

Proposition. *La définition donnée ci-dessus de la relation $(\leqslant)$ est correcte. C'est-à-dire, quels que soient six nombres naturels a_1, a_2, b_1, b_2, c_1, c_2, si $b_1 - a_1 = b_2 - a_2$ et $c_1 - a_1 = c_2 - a_2$, alors*

$$b_1 \leqslant c_1 \quad \Leftrightarrow \quad b_2 \leqslant c_2.$$

Démonstration. Soient a_1, a_2, b_1, b_2, c_1, c_2 six nombres naturels tels que $b_1 - a_1 = b_2 - a_2$ et $c_1 - a_1 = c_2 - a_2$. Alors,

$$(a_1,b_1) \mathrel{\underset{+}{=}} (a_2,b_2) \quad \text{et} \quad (a_1,c_1) \mathrel{\underset{+}{=}} (a_2,c_2)$$

(voir la définition des *entiers relatifs*), c'est-à-dire,

$$b_1 + a_2 = b_2 + a_1 \quad \text{et} \quad c_1 + a_2 = c_2 + a_1.$$

D'après les propriétés des nombres naturels déjà établies,

$$\begin{aligned} b_1 \leqslant c_1 \quad &\Leftrightarrow \quad b_1 + a_2 \leqslant c_1 + a_2 \\ &\Leftrightarrow \quad b_2 + a_1 \leqslant c_2 + a_1 \quad \Leftrightarrow \quad b_2 \leqslant c_2. \end{aligned}$$

□

Exercice. Vérifier si les définitions des relations $(\geqslant)$, $(<)$, $(>)$ sont correctes elles aussi.

Proposition. *Les définitions données ci-dessus des relations $(\leqslant)$, $(\geqslant)$, $(<)$, $(>)$ sont toutes complètes. C'est-à-dire, quels que soient deux entiers x et y, il existe trois nombres naturels a, b, c tels que $x = b - a$ et $y = c - a$.*

Démonstration. Soient x et y deux nombres entiers arbitraires. Soient a, b, c, d nombres naturels tels que $x = a - b$ et $y = c - d$. Alors

$$x = (a + d) - (b + d), \qquad y = (c + b) - (b + d). \qquad \square$$

Exercice. Essayons de définir une relation (Δ) entre des nombres naturels par l'équivalence suivante :

$$a + b \,\Delta\, c + d \quad \Leftrightarrow \quad b + c = d + a.$$

Est-ce que cette tentative définition est correcte ?

Proposition. *Quels que soient les nombres naturels a, b, c, d, les équivalences suivantes sont satisfaites* :

$$\begin{aligned}
a - b \leqslant c - d \quad &\Leftrightarrow \quad a + d \leqslant c + b,\\
a - b \geqslant c - d \quad &\Leftrightarrow \quad a + d \geqslant c + b,\\
a - b < c - d \quad &\Leftrightarrow \quad a + d < c + b,\\
a - b > c - d \quad &\Leftrightarrow \quad a + d > c + b.
\end{aligned}$$

Démonstration. Comme $a - b = (a + d) - (b + d)$ et $c - d = (c + b) - (d + b)$, on a :

$$\begin{aligned}
& a - b \leqslant c - d\\
\Leftrightarrow \quad & (a + d) - (b + d) \leqslant (c + b) - (d + b)\\
\Leftrightarrow \quad & a + d \leqslant c + b.
\end{aligned}$$

On vérifie de la même manière les cas de $(\geqslant)$, de $(<)$ et de $(>)$. $\square$

Les relations $(\leqslant)$, $(\geqslant)$, $(<)$, $(>)$ sont reliées par les équivalences suivantes :

(1) $x \leqslant y$ si et seulement si $y \geqslant x$,

(2) $x < y$ si et seulement si $y > x$,

(3) $x \leqslant y$ si et seulement si $x < y$ ou $x = y$,

(4) $x < y$ si et seulement si $x \leqslant y$ et $x \neq y$.

Exercice. Vérifier ces équivalences.

Les quatre propriétés suivantes de la relation $(\leqslant)$ entre des nombres entiers sont les mêmes que pour la relation $(\leqslant)$ entre des nombres naturels :

(1) si $x \leqslant y$ et $y \leqslant z$, alors $x \leqslant z$,

(2) $x \leqslant x$,

(3) si $x \leqslant y$ et $y \leqslant x$, alors $x = y$,

(4) $x \leqslant y$ ou $y \leqslant x$.

Exercice. Démontrer ces propriétés.

Les trois propriétés suivantes de la relation $(<)$ entre des nombres entiers sont les mêmes que pour la relation $(<)$ entre des nombres naturels :

(1) si $x < y$ et $y < z$, alors $x < z$,

(2) si $x < y$, alors $x \neq y$,

(3) si $x \neq y$, alors $x < y$ ou $y < x$.

Exercice. Démontrer ces propriétés.

Notation. Si x et y sont deux entiers, on va noter « $\max(x, y)$ » le plus grand entre x et y et « $\min(x, y)$ » le plus petit entre x et y :

$$\max(x, y) \overset{\text{déf}}{=} \begin{cases} x & \text{si} \quad x \geqslant y, \\ y & \text{si} \quad x \leqslant y; \end{cases} \qquad \min(x, y) \overset{\text{déf}}{=} \begin{cases} x & \text{si} \quad x \leqslant y, \\ y & \text{si} \quad x \geqslant y. \end{cases}$$

Entiers positifs et négatifs

Définition. Soient a et b deux nombres naturels. Le nombre entier $b - a$ est dit :

(1) *positif* (au sens large) si et seulement si $a \leqslant b$,

(2) *négatif* (au sens large) si et seulement si $a \geqslant b$,

(3) *strictement positif* si et seulement si $a < b$,

(4) *strictement négatif* si et seulement si $a > b$.

Autrement dit,

(1) x est *positif* (au sens large) si et seulement si $x \geqslant 0$,

(2) x est *négatif* (au sens large) si et seulement si $x \leqslant 0$,

(3) x est *strictement positif* si et seulement si $x > 0$,

(4) x est *strictement négatif* si et seulement si $x < 0$.

Ainsi, les entiers positifs (au sens large) sont les nombres naturels, et tout entier négatif peut être écrit sous la forme « $-a$ », où a est un nombre naturel.

II.3. « Translation additive » d'un nombre naturel par un entier relatif

En introduisant les nombres entiers relatifs, on a *prolongé* l'opération de soustraction des nombres naturels pour que la valeur de la différence « $a - b$ » soit définie quels que soient les nombres naturels a et b (même quand $a < b$), et on a défini les nombres entiers

comme les valeurs de toutes les différences entre des nombres naturels. Cependant, pour l'instant, les opérations d'addition, de soustraction, de multiplication et de division ne sont définies que pour les nombres naturels.

Dans la section suivante on va chercher une façon convenable de prolonger l'opération d'addition des nombres naturels en une opération définies pour n'importe quels entiers relatifs, qu'on va toujours appeler l'*addition* et noter « $+$ ».

Pour commencer, on va adopter la définition suivante, qui paraît tout à fait naturelle.

Définition. Si a et b sont deux nombres naturels, et que $x = b - a$, alors la *somme* de a et de l'entier x, notée « $a + x$ », est b :

$$a + (b - a) \stackrel{\text{déf}}{=} b.$$

Cette définition est clairement en accord avec la définition de l'addition des nombres naturels, car si a, b et $b - a$ sont tous nombres naturels, alors la somme de a et $b - a$ est b, au sens de l'addition des nombres naturels. Ainsi, cette définition, pourvu qu'elle soit correcte, *prolonge* l'opération d'addition des nombres naturels.

Il est facile de montrer que cette définition est correcte, c'est-à-dire, que si a est un nombre naturel et x est un entier relatif tels que la définition s'applique pour donner une valeur de « $a + x$ », alors elle ne donnera qu'une valeur unique. En effet : si b_1 et b_2 sont deux nombres naturels tels que $x = b_1 - a = b_2 - a$, alors $b_1 = b_2$, d'après un lemme précédent.

Exemple. $5 + (-3) = 5 + (0 - 3) = 5 + (2 - 5) = 2$.

Exercice. Calculer et simplifier : $1 + (-1)$.

Cependant, la valeur de « $3 + (0 - 5)$ » n'est pas encore définie.

Soit x un entier. Si a et b sont deux nombres naturels tels que $x = b - a$, alors on va, de manière informelle, appeler $b = a + x$ le *« translaté additif »* de a par x. On peut parler de l'opération de *« translation additive »* par x, qui a certains nombres naturels associe leurs translatés additifs par x.

II.4. Addition

D'après la définition de la « translation additive », quels que soient trois nombres naturels a, b, c, on a :

$$a + (b - a) + (c - b) = b + (c - b) = c = a + (c - a).$$

Cette observation suggère qu'il est naturel de définir l'opération d'*addition* $(+)$ des entiers relatifs de telle manière que pour tous nombres naturels a, b, c, on ait l'égalité :

$$(b - a) + (c - b) = c - a.$$

Pour voir si on peut imposer cette identité comme la définition de l'addition d'entiers, il suffit de vérifier si pour tous nombres naturels a_1, a_2, b_1, b_2, c_1, c_2 tels que $b_1 - a_1 = b_2 - a_2$ et $c_1 - b_1 = c_2 - b_2$, on a $c_1 - a_1 = c_2 - a_2$. D'après le lemme suivant, c'est le cas.

Lemme. *Soient six nombres naturels* a_1, a_2, b_1, b_2, c_1, c_2 *tels que* $(a_1, b_1) \mathrel{\underset{+}{\simeq}} (a_2, b_2)$ *et* $(b_1, c_1) \mathrel{\underset{+}{\simeq}} (b_2, c_2)$. *Alors* $(a_1, c_1) \mathrel{\underset{+}{\simeq}} (a_2, c_2)$.

Démonstration. Comme $(a_1, b_1) \mathrel{\underset{+}{\simeq}} (a_2, b_2)$, on en déduit que $(a_1, a_2) \mathrel{\underset{+}{\simeq}} (b_1, b_2)$. Comme $(b_1, c_1) \mathrel{\underset{+}{\simeq}} (b_2, c_2)$, on en déduit que $(b_1, b_2) \mathrel{\underset{+}{\simeq}} (c_1, c_2)$. Ainsi, $(a_1, a_2) \mathrel{\underset{+}{\simeq}} (c_1, c_2)$. D'où, $(a_1, c_1) \mathrel{\underset{+}{\simeq}} (a_2, c_2)$. □

Définition. Si a, b, c sont trois nombres naturels, $x = b - a$ et $y = c - b$, alors la *somme* des entiers x et y, notée « $x + y$ », est $c - a$:

$$(b - a) + (c - b) \stackrel{\text{déf}}{=} c - a.$$

Exercice. Montrer, en utilisant le dernier lemme, que cette définition est correcte. Vérifier en plus qu'elle est complète, c'est-à-dire, qu'elle définit la somme de deux n'importe quels entiers.

Ainsi on a défini l'opération d'*addition* $(+)$ qui à deux n'importe quels entiers associe leur somme.

Exemples.

$$\begin{aligned}
&(3 - 1) + (9 - 4) = (3 - 1) + (8 - 3) = 8 - 1 = 7,\\
&(3 - 1) + (4 - 9) = (9 - 7) + (4 - 9) = 4 - 7 = 0 - 3 = -3,\\
&(1 - 3) + (9 - 4) = (1 - 3) + (6 - 1) = 6 - 3 = 3,\\
&(1 - 3) + (4 - 9) = (5 - 7) + (0 - 5) = 0 - 7 = -7.
\end{aligned}$$

Exercice. Calculer et simplifier : $(-1) + 1$, $1 + (-1)$, $(-1) + (-1)$.

En général, pour tous nombres naturels a, b, c, d,

$$\begin{aligned}
(a - b) + (c - d) &= ((a + d) - (b + d)) + ((a + c) - (a + d))\\
&= (a + c) - (b + d).
\end{aligned}$$

Exercice. Essayons de définir une opération (Δ) sur des nombres naturels par l'identité suivante :

$$(a + b) \,\Delta\, (c + d) \stackrel{\text{déf}}{=} ab + cd.$$

Est-ce que cette tentative définition est correcte ?

Les trois identités suivantes satisfaites par l'opération d'addition de nombres entiers sont les mêmes que pour l'opération d'addition de nombres naturels :

(1) $x + (y + z) = (x + y) + z$,

(2) $x + 0 = x = 0 + x$,

(3) $y + x = x + y$.

Exercice. Démontrer ces identités.

Notation. On adopte une écriture abrégée pour les sommes de la forme « $0 + x$ » : au lieu de « $0 + x$ », on peut écrire « $+x$ ».

Exemple. L'expression « $+(+(+42))$ » veut dire $0 + (0 + (0 + 42))$.

Lemme. *Soit x un entier arbitraire. Soient a et b deux nombres naturels tels que $x = b - a$. Posons $y = a - b$. Alors $x + y = 0 = y + x$.*

Exercice. Prouver ce lemme.

Proposition. *Pour tous entiers x et y, il existe un unique entier z tel que $z + y = x$.*

Démonstration. Soient x et y deux entiers arbitraires, et soit v un entier tel que $y + v = v + y = 0$ (il existe d'après le lemme précédent). Alors

$$(x + v) + y = x + (v + y) = x + 0 = x.$$

On a montré l'existence, il reste à montrer l'unicité : que si z est un entier tel que $z + y = x$, alors $z = x + v$.

Soit z un entier tel que $z + y = x$. Alors

$$z = z + 0 = z + (y + v) = (z + y) + v = x + v. \qquad \square$$

Définition. Deux entiers x et y sont dits *opposés* l'un de l'autre si et seulement si $x + y = 0$.

Rapport aux relations d'ordre usuelles

Proposition. *Pour tous entiers x, y, z, si $x < y$, alors $x + z < y + z$.*

Exercice. Prouver cette proposition.

Corollaire. *Pour tous entiers x, y, z, les équivalences suivantes sont satisfaites* :

$$x < y \quad \Leftrightarrow \quad x + z < y + z, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad x + z \leqslant y + z.$$

Exercice. Prouver ce corollaire.

II.5. Soustraction

La définition de l'opération de *soustraction* repose sur les propriétés suivantes des nombres entiers :

(1) si $y + x = z + x$, alors $y = z$,

(2) quels que soient x et y, il existe z tel que $z + x = y$.

Soient x et y deux entiers. On peut tenter de chercher un entier z tel que $z + x = y$. Comme montré précédemment, il y en a un, et un seul.

Définition. Si x et y sont deux entiers, alors l'unique entier z tel que $z + x = y$ est dit la *différence* de y et x et est noté « $y - x$ ».

Ainsi on a défini l'opération de *soustraction* $(-)$ qui à deux n'importe quels entiers associe leur différence.

Exercice. Calculer et simplifier : $(-1) - 1$, $1 - (-1)$, $(-1) - (-1)$.

La définition de l'opération de soustraction $(-)$ donnée ci-dessus peut être exprimée par l'équivalence suivante :

$$y - x = z \quad \Leftrightarrow \quad y = z + x.$$

L'opération de soustraction $(-)$ d'entiers peut aussi être définie par les deux identités suivantes, à la condition que l'opération d'addition $(+)$ est déjà définie :

(1) $(x + y) - y = x$, (2) $(x - y) + y = x$.

En fait, n'importe quelle de ces deux identités suffit toute seule pour définir l'opération de soustraction d'entiers.

Exercice. Montrer que n'importe quelle de ces deux identités suffit toute seule pour définir l'opération de soustraction d'entiers.

Exercice. Soient a, b, c, d quatre nombres naturels. Montrer que

$$(a - b) - (c - d) = (a + d) - (b + c).$$

Les identités suivantes sont satisfaites (pour tous x, y, z entiers) :

(1) $x + (y - z) = (x + y) - z$,

(2) $x - (y + z) = (x - z) - y$,

(3) $x - (y - z) = (x + z) - y$,

(4) $(x - y) + (y - z) = x - z$,

(5) $(x + z) - (y + z) = x - y$,

(6) $(x - y) + z = (x + z) - y$,

(7) $(x - y) - z = (x - z) - y$,

(8) $x - (x - y) = y$,

(9) $x - 0 = x$,

(10) $x - x = 0$.

Exercice. Démontrer ces identités.

Notation. On adopte une écriture abrégée pour les différences de la forme « $0 - x$ » : au lieu de « $0 - x$ », on peut écrire « $-x$ ».

Exemple. L'expression « $-(-(-42))$ » veut dire $0 - (0 - (0 - 42))$.

Observons que :

(1) $-(-x) = 0 - (0 - x) = x$,

(2) $x + (-y) = x + (0 - y) = (x + 0) - y = x - y$.

Rapport aux relations d'ordre usuelles

Proposition. *Pour tous entiers x, y, z, si $x < y$, alors $z - x > z - y$.*

Exercice. Prouver cette proposition.

Corollaire. *Pour tous entiers x, y, z, les équivalences suivantes sont satisfaites* :

$$x < y \quad \Leftrightarrow \quad z - x > z - y, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad z - x \geqslant z - y.$$

En particulier :

(1) x est strictement positif si et seulement si $-x$ est strictement négatif,

(2) x est strictement négatif si et seulement si $-x$ est strictement positif,

(3) x est positif (au sens large) si et seulement si $-x$ est négatif (au sens large),

(4) x est négatif (au sens large) si et seulement si $-x$ est positif (au sens large).

Exercice. Prouver le dernier corollaire.

II.6. Multiplication

Définition. Si a est un nombre naturel et x est un entier, alors le *produit* de x et a, noté « $x \times a$ », « $x \cdot a$ », ou « xa », est défini par la règle :

$$xa \overset{\text{déf}}{=} 0 \underbrace{+ x + x + \cdots + x}_{a \text{ fois}}.$$

Lemme. *Pour tous a, b, c naturels, $(a - b)c = ac - bc$.*

L'identité $(a - b)c = ac - bc$ est déjà établie dans le cas où tous les nombres qui interviennent dans le calcul sont naturels, c'est-à-dire, dans le cas où $b \leqslant a$. Il reste à vérifier le cas général.

Démonstration du lemme. D'après les propriétés de l'addition et de la soustraction déjà établies,

$$\begin{aligned}
(a-b)c &= 0 \underbrace{+ (a-b) + (a-b) + \cdots + (a-b)}_{c \text{ fois}} \\
&= 0 \underbrace{+ (a + (-b)) + (a + (-b)) + \cdots + (a + (-b))}_{c \text{ fois}} \\
&= 0 \underbrace{+ a + a + \cdots + a}_{c \text{ fois}} \underbrace{+ (-b) + (-b) + \cdots + (-b)}_{c \text{ fois}} \\
&= 0 \underbrace{+ a + a + \cdots + a}_{c \text{ fois}} - (0 \underbrace{+ b + b + \cdots + b}_{c \text{ fois}}) \\
&= ac - bc. \qquad \square
\end{aligned}$$

Définition. Si a et b sont deux nombres naturels, x est un entier, et $y = b - a$, alors le *produit* de x et y, noté « $x \times y$ », « $x \cdot y$ », ou « xy », est défini par la règle :

$$\begin{aligned}
x(b-a) &\overset{\text{déf}}{=} 0 \underbrace{+ x + x + \cdots + x}_{b \text{ fois}} \underbrace{- x - x - \cdots - x}_{a \text{ fois}} \\
&= 0 \underbrace{+ x + x + \cdots + x}_{b \text{ fois}} - (0 \underbrace{+ x + x + \cdots + x}_{a \text{ fois}}) = xb - xa.
\end{aligned}$$

Exercice. Vérifier si cette définition est correcte.

Ainsi on a défini l'opération de *multiplication* $(\cdot)$ (aussi notée « $(\times)$ ») qui à deux n'importe quels entiers associe leur produit.

Exercice. Calculer $(-1)1$, $1(-1)$ et $(-1)(-1)$.

Proposition. *Pour tous entiers x et y, $yx = xy$.*

Démonstration. Soient x et y deux entiers arbitraires. Soient a, b, c, d quatre nombres naturels tels que $a - b = x$ et $c - d = y$. Alors, en appliquant le dernier lemme et d'autres propriétés déjà établies, on trouve :

$$\begin{aligned}
xy &= x(c-d) = xc - xd = (a-b)c - (a-b)d = (ac - bc) - (ad - bd) \\
&= ac - bc + bd - ad = ca - cb + db - da = ca - da + db - cb \\
&= (ca - da) - (cb - db) = (c-d)a - (c-d)b = ya - yb = y(a-b) \\
&= yx. \qquad \square
\end{aligned}$$

Les identités suivantes sont satisfaites :

(1) $x(yz) = (xy)z$,

(2) $x \cdot 1 = x = 1 \cdot x$,

(3) $yx = xy$,

(4) $x(y + z) = xy + xz$,

(5) $x(y - z) = xy - xz$,

(6) $x \cdot 0 = 0$.

Exercice. Démontrer ces identités.

Rapport aux relations d'ordre usuelles

Proposition. *Pour tous entiers x, y, z,*

(1) *si $x < y$ et $z > 0$, alors $xz < yz$,*

(2) *si $x < y$ et $z < 0$, alors $xz > yz$.*

Exercice. Prouver cette proposition.

Corollaire. *Pour tous entiers x, y, z,*

(1) *si $z > 0$, alors les équivalences suivantes sont satisfaites* :

$$x < y \quad \Leftrightarrow \quad xz < yz, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad xz \leqslant yz,$$

(2) *si $z < 0$, alors les équivalences suivantes sont satisfaites* :

$$x < y \quad \Leftrightarrow \quad xz > yz, \qquad\qquad x \leqslant y \quad \Leftrightarrow \quad xz \geqslant yz.$$

Exercice. Prouver ce corollaire.

Corollaire. *Si x, y, z sont trois entiers tels que $xz = yz$ et que $z \neq 0$, alors $x = y$.*

Exercice. Prouver ce corollaire.

Corollaire. *Pour tous entiers x et y,*

(1) *si $x > 0$ et $y > 0$, alors $xy > 0$,*

(2) *si $x > 0$ et $y < 0$, alors $xy < 0$,*

(3) *si $x < 0$ et $y > 0$, alors $xy < 0$,*

(4) *si $x < 0$ et $y < 0$, alors $xy > 0$.*

Exercice. Prouver ce corollaire.

Corollaire. *Si x et y sont deux entiers tels que $x \neq 0$ et $y \neq 0$, alors $xy \neq 0$.*

Exercice. Prouver ce corollaire.

Corollaire. *Pour tout entier x, $xx \geqslant 0$.*

Exercice. Prouver ce corollaire.

Exercice. Trouver tous les nombres entiers x tels que $xx + 5x + 4 < 0$. Indication : $xx + 5x + 4 = xx + x + 4x + 4 = (x + 1)(x + 4)$.

Multiplication par un nombre non nul

Les deux propositions suivantes ont été présentées ci-dessus comme corollaires de propriétés de la multiplication en rapport avec les relations d'ordre, mais elles méritent d'être contemplées indépendamment des relations d'ordre.

Proposition. *Si x, y, z sont trois entiers tels que $xz = yz$ et que $z \neq 0$, alors $x = y$.*

Proposition. *Si x et y sont deux entiers tels que $x \neq 0$ et $y \neq 0$, alors $xy \neq 0$.*

Exercice. Trouver tous les nombres entiers x tels que $xx + 5x + 4 = 0$. Indication : $xx + 5x + 4 = xx + x + 4x + 4 = (x + 1)(x + 4)$.

II.7. Valeur absolue

Définition. Si a et b sont deux nombres naturels, et que $x = b - a$, alors la *valeur absolue* de l'entier x, notée « $|x|$ », est définie ainsi :

$$|b - a| \overset{\text{déf}}{=} \begin{cases} b - a & \text{si} \quad a \leqslant b, \\ a - b & \text{si} \quad b \leqslant a. \end{cases}$$

Autrement dit, si x est un entier, alors

$$|x| \overset{\text{déf}}{=} \begin{cases} +x & \text{si} \quad x \geqslant 0, \\ -x & \text{si} \quad x \leqslant 0. \end{cases}$$

Ainsi, la valeur absolue de tout entier est positive (au sens large).

En utilisant la notation avec « max », on peut définir la valeur absolue d'un entier x par la formule :

$$|x| = \max(x, -x).$$

Une autre façon (équivalente) de définir la valeur absolue d'un entier x est par l'équivalence suivante :

$$|x| = y \quad \Leftrightarrow \quad \begin{cases} y \geqslant 0 \\ xx = yy \end{cases}.$$

Exercice. Montrer que la valeur absolue peut être définie par cette équivalence. Indication : si a et b sont deux nombres naturels tels que $aa = bb$, alors $a = b$, car, pour les nombres naturels a et b, si $a < b$, alors $aa < bb$.

Lemme. *Pour tous entiers x et y,*

$$\begin{aligned} |x| \leqslant y \quad &\Leftrightarrow \quad -y \leqslant x \leqslant y, \\ |x| < y \quad &\Leftrightarrow \quad -y < x < y. \end{aligned}$$

Démonstration.

$$\begin{aligned} |x| \leqslant y \quad &\Leftrightarrow \quad \max(x, -x) \leqslant y \quad \Leftrightarrow \quad \begin{cases} x \leqslant y \\ -x \leqslant y \end{cases} \\ &\Leftrightarrow \quad \begin{cases} x \leqslant y \\ -y \leqslant x \end{cases} \quad \Leftrightarrow \quad -y \leqslant x \leqslant y, \\ |x| < y \quad &\Leftrightarrow \quad \max(x, -x) < y \quad \Leftrightarrow \quad \begin{cases} x < y \\ -x < y \end{cases} \\ &\Leftrightarrow \quad \begin{cases} x < y \\ -y < x \end{cases} \quad \Leftrightarrow \quad -y < x < y. \end{aligned}$$

□

Proposition (Inégalité triangulaire)**.** *Pour tous entiers x et y,*

$$|x+y| \leqslant |x| + |y|\,.$$

Démonstration. Comme $|x| \leqslant |x|$ et $|y| \leqslant |y|$, d'après le lemme précédent on a :

$$-|x| \leqslant x \leqslant |x| \quad \text{et} \quad -|y| \leqslant y \leqslant |y|\,.$$

D'où,

$$-(|x| + |y|) \leqslant x + y \leqslant |x| + |y|\,,$$

et donc, encore d'après le lemme précédent,

$$|x+y| \leqslant |x| + |y|\,. \qquad \square$$

L'origine du nom « *inégalité triangulaire* » sera peut-être plus claire si l'on traduit cette inégalité sous la forme suivante :

$$|c-a| \leqslant |b-a| + |c-b|\,.$$

Proposition. *Pour tous entiers x et y,*

$$|xy| = |x|\,|y|\,.$$

Démonstration. Soient x et y deux entiers arbitraires. Alors

$$(xy)(xy) = (xx)(yy) = (|x|\,|x|)(|y|\,|y|) = (|x|\,|y|)(|x|\,|y|),$$

et $|x|\,|y| \geqslant 0$. D'où, $|xy| = |x|\,|y|$, d'après une des définitions équivalentes de la valeur absolue. $\square$

II.8. Divisibilité

Définition. On dit qu'un entier x *divise* un entier y si et seulement si il existe un entier z tel que $y = xz$.

Exercice. Vu que l'ensemble des nombres naturels fait partie de l'ensemble des entiers, maintenant on a deux définitions de la divisibilité pour les nombres naturels. Selon l'ancienne, a divise b si et seulement si il existe un nombre naturel c tel que $b = ac$. Selon la nouvelle, a divise b si et seulement si il existe un entier z tel que $b = az$. Vérifier qu'il n'y a pas de contradiction entre les deux définitions.

Exemples. Les entiers 2, -3 et 4 divisent -12, mais 5 ne le divise pas. Tout entier divise 0. Le nombre 0 ne divise que lui-même. Les nombres 1 et -1 divisent tous les entiers.

Notation. On utilise toujours la notation « $x \mid y$ » pour dire « x divise y ».

Ainsi on a défini la *relation de divisibilité* (|) entre entiers.

Au lieu de dire que x divise y, on peut dire que y *se factorise* par x, ou encore que x est un *diviseur* de y, ou que y est un *multiple* de x. Voici donc quatre façons différentes d'exprimer une même relation entre x et y, notée « $x \mid y$ » :

(1) x divise y,
(2) y se factorise par x,
(3) x est diviseur de y,
(4) y est multiple de x.

Exemples. L'entier 3 est diviseur de -12, et -12 est multiple de 3.

Définition. Les entiers qui sont multiples de 2 sont dits *pairs*, et les autres sont dits *impairs*.

Lemme. *Pour tous entiers x et y, x divise y si et seulement si $|x|$ divise $|y|$.*

Exercice. Prouver le lemme.

Les deux propriétés suivantes de la relation (|) entre des nombres entiers sont les mêmes que pour la relation (|) entre des nombres naturels :

(1) si $x \mid y$ et $y \mid z$, alors $x \mid z$,
(2) $x \mid x$.

Exercice. Démontrer les deux propriétés.

Cependant, il n'est pas vrai en général que si $x \mid y$ et $y \mid x$, alors $x = y$. Ce qui est vrai, en revanche, c'est que si $x \mid y$ et $y \mid x$, alors $|x| = |y|$.[1]

Définition. Deux entiers sont dits *premiers entre eux* si et seulement si tout leur diviseur commun divise 1. Au lieu de dire que a et b sont premiers entre eux, on peut aussi dire que a est *premier avec* b.

Autrement dit, deux entiers sont premiers entre eux si et seulement si ils n'ont pas de diviseurs communs autres que 1 et -1.

Exemples. Les entiers -10 et -21 sont premiers entre eux, mais -10 et 15 ne le sont pas.

Proposition. *Soient x, y, z trois entiers tels que z divise x et y. Alors z divise $x+y$, ainsi que $x-y$.*

Exercice. Prouver cette proposition.

[1] Parfois on utilise la définition suivante : deux entiers sont dits *associés* (entre eux) si et seulement chacun des deux divise l'autre. Ainsi, deux entiers x et y sont associés si et seulement si $x = y$ ou $x = -y$.

II.9. Division

La définition de l'opération de *division* repose sur la propriété suivante des nombres entiers :

si $yx = zx$ et $x \neq 0$, alors $y = x$.

Soient x et y deux entiers. On peut tenter de chercher un entier z tel que $zx = y$. Si $x \nmid y$, il n'y en a pas. Si $x = y = 0$, alors tout valeur de « z » convient. Si $x \neq 0$ et que $x \mid y$, alors il y a un et un seul entier z tel que $zx = y$.

Définition. Si x est un entier non nul et y est un multiple de x, alors l'unique entier z tel que $zx = y$ est dit le *quotient* de y par x et est noté « $y \div x$ », ou « $y : x$ », ou « y/x », ou « $x\backslash y$ », ou « $\dfrac{y}{x}$ ». Dans les autres cas, aucun entier n'est dit « quotient de y par x ».

Ainsi on a défini l'opération de *division* ($/$) qui à deux entiers associe leur quotient, tant que leur quotient est défini.

Exemples. $12/(-3) = -4$, mais on n'a pas défini la valeur de l'expression « $12/5$ », ni la valeur de l'expression « $12/0$ », ni la valeur de l'expression « $0/0$ », comme un entier.

Exercice. Calculer $(-1)/1$, $1/(-1)$ et $(-1)/(-1)$.

La définition de l'opération de division donnée ci-dessus peut être exprimée par l'équivalence suivante :

$$\frac{y}{x} = z \quad \Leftrightarrow \quad \begin{cases} x \neq 0 \\ y = zx \end{cases}.$$

L'opération de division ($/$) d'entiers peut aussi être définie par les trois propriétés suivantes, à la condition que l'opération de multiplication ($\cdot$) est déjà définie :

(1) $(xy)/y = x$ si $y \neq 0$,

(2) $(x/y)y = x$ si $y \neq 0$ et $y \mid x$,

(3) la valeur de « x/y » n'est définie (comme un nombre entier) que si $y \neq 0$ et $y \mid x$.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.

Exercice. Montrer que la deuxième propriété résulte de la première, et que la première résulte de la deuxième.

Voici quelques identités remarquables satisfaites par l'opération de division (pour les entiers) :

(1) $x(y/z) = (xy)/z$ si $z \mid y$ et $z \neq 0$,

(2) $x/(yz) = (x/z)/y$ si $yz \mid x$ et $yz \neq 0$,

(3) $x/(y/z) = (xz)/y$ si $z \mid y \mid xz$ et $y \neq 0$,

(4) $(x/y)(y/z) = x/z$ si $z \mid y \mid x$ et $y \neq 0$,

(5) $(xz)/(yz) = x/y$ si $y \mid x$ et $yz \neq 0$,

(6) $(x/y)z = (xz)/y$ si $y \mid x$ et $y \neq 0$,

(7) $(x/y)/z = (x/z)/y$ si $yz \mid x$ et $yz \neq 0$,

(8) $x/(x/y) = y$ si $y \mid x$ et $x \neq 0$,

(9) $x/1 = x$,

(10) $x/x = 1$ si $x \neq 0$,

(11) $(x+y)/z = x/z + y/z$ si $z \mid x$, $z \mid y$ et $z \neq 0$,

(12) $(x-y)/z = x/z - y/z$ si $z \mid x$, $z \mid y$ et $z \neq 0$,

(13) $0/x = 0$ si $x \neq 0$.

Exercice. Démontrer ces identités.

II.10. Exponentiation, puissances

Définition. Si a est un nombre naturel et x est un entier, alors x *puissance* a, ou la a-ième *puissance* de x, ou x *élevé à la* a*-ième puissance*, est le nombre noté « x^a » et défini par la règle :

$$x^a \overset{\text{déf}}{=} 1 \underbrace{\cdot\, x \cdot x \cdot \cdots \cdot x}_{a \text{ fois}}.$$

Les identités suivantes sont satisfaites pour tous a et b naturels et pour tous x et y entiers :

(1) $x^{ab} = (x^a)^b$,

(2) $x^1 = x$,

(3) $x^{a+b} = x^a x^b$,

(4) $x^{a-b} = x^a/x^b$ si $x \neq 0$ et $b \leqslant a$,

(5) $x^0 = 1$,

(6) $(xy)^a = x^a y^a$,

(7) $(x/y)^a = x^a/y^a$ si $y \neq 0$ et $y \mid x$,

(8) $1^a = 1$.

Exercice. Démontrer ces identités.

Définition. Si a et b sont deux nombres naturels, u est un diviseur entier de 1 (autrement dit, $u = \pm 1$), et $x = b - a$, alors u *puissance* x est le nombre noté « u^x » et défini par la règle :

$$u^{b-a} \overset{\text{déf}}{=} 1 \underbrace{\cdot u \cdot u \cdot \cdots \cdot u}_{b \text{ fois}} \underbrace{/u/u/\cdots/u}_{a \text{ fois}} = \frac{u^b}{u^a}.$$

Exercice. Vérifier si cette définition est correcte.

Exercice. Calculer 1^{-1} et $(-1)^{-1}$.

II.11. Racines

Définition. Une *racine carrée* d'un nombre x est un nombre y tel que $y^2 = x$. Une *racine cubique* d'un nombre x est un nombre y tel que $y^3 = x$. En général, si n est un nombre naturel non nul, une *racine n-ième* d'un nombre x est un nombre y tel que $y^n = x$.

Exemples. Le nombre -3 est une racine carré de 9, 2 est une racine cubique de 8, -1 est une racine 2023-ième de -1.

Exercice. Montrer que pour tout nombre naturel non nul n, 0 est l'unique racine n-ième de 0.

Exercice. Montrer que si n est un nombre naturel non nul pair et x est un entier strictement négatif, alors parmi les nombres entiers[2] il n'y a pas de racines n-ièmes de x.

Proposition. (1) *Si u est une racine n-ième de x et v est une racine n-ième de y, alors uv est une racine n-ième de xy.*

(2) *Si x est une racine m-ième de y et y est une racine n-ième de z, alors x est une racine mn-ième de z.*

Exercice. Prouver cette propositions.

Proposition. (1) *Si x est une racine carrée de y, alors $-x$ l'est aussi.*

(2) *Si x et y sont deux racines carrées de z, alors $y = x$ ou $y = -x$.*

Exercice. Prouver cette propositions. Indication : pour la deuxième partie, considérer le produit $(x + y)(x - y)$.

Proposition. *Si n est un nombre naturel non nul et x et y sont deux entiers positifs tels que $x^n = y^n$, alors $x = y$.*

[2] On peut montrer qu'il n'y en a pas parmi les *nombres réels* non plus. En revanche, parmi les *nombres complexes* il y en a n.

Exercice. Prouver cette propositions.

Proposition. *Si n est un nombre naturel impair et x et y sont deux entiers tels que $x^n = y^n$, alors $x = y$.*

Exercice. Prouver cette propositions.

Définition. Soient n un nombre naturel impair et x un entier qui est la n-ième puissance d'un entier y ($x = y^n$). Alors ***la*** racine n-ième de x est l'unique racine n-ième entière de x (donc y).

Définition. Soient n un nombre naturel non nul et x un entier positif ($x \geqslant 0$) qui est la n-ième puissance d'un entier y ($x = y^n$). Alors ***la*** racine n-ième de x est l'unique racine n-ième positive de x (donc $|y|$). Si x est strictement positif ($x > 0$), alors la racine n-ième positive de x est aussi dite la racine n-ième *principale* de x.

Notation. Si n est un nombre naturel non nul et x est un entier qui admet une racine n-ième entière[3], alors on note « $\sqrt[n]{x}$ » ou « $\sqrt[n]{x}$ » l'unique racine n-ième entière de x si n et impair, et on note « $\sqrt[n]{x}$ » ou « $\sqrt[n]{x}$ » l'unique racine n-ième positive de x si n est pair. Si n est pair et x est strictement négatif, alors la valeur de l'expression « $\sqrt[n]{x}$ » n'est pas définie (l'expression « $\sqrt[n]{x}$ » n'a pas de sens). Dans le cas où $n = 2$, on utilise aussi la notation « $\sqrt{x}$ » au lieu de « $\sqrt[2]{x}$ ».

Ainsi, si n est un nombre naturel *impair*, alors pour tous x et y entiers,

$$\sqrt[n]{x} = y \quad \Leftrightarrow \quad x = y^n,$$

et si n est un nombre naturel non nul *pair*, alors pour tous x et y entiers,

$$\sqrt[n]{x} = y \quad \Leftrightarrow \quad \begin{cases} y \geqslant 0 \\ x = y^n \end{cases}.$$

Pour n naturel *impair*, l'opération $\sqrt[n]{}$ sur les entiers peut aussi être définie par les trois propriétés suivantes :

(1) $\sqrt[n]{x^n} = x$,

(2) $(\sqrt[n]{x})^n = x$ si x est la n-ième puissance d'un entier,

(3) la valeur de « $\sqrt[n]{x}$ » n'est définie (comme un nombre entier) que si x est la n-ième puissance d'un entier.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.

Pour n naturel non nul *pair*, l'opération $\sqrt[n]{}$ sur les entiers peut aussi être définie par les trois propriétés suivantes :

[3] La même notation sera utilisée pour les racines *réelles*.

(1) $\sqrt[n]{x^n} = x$ si $x \geqslant 0$,

(2) $(\sqrt[n]{x})^n = x$ si x est la n-ième puissance d'un entier,

(3) la valeur de « $\sqrt[n]{x}$ » n'est définie (comme un nombre entier) que si x est la n-ième puissance d'un entier.

En fait, la deuxième propriété résulte de la première, et la première résulte de la deuxième, donc il suffit de garder une seule parmi les deux.

Exemples. $\sqrt{9} = 3$, $\sqrt[3]{-8} = -2$, $\sqrt[1000]{0} = 0$, $\sqrt[2023]{-1} = -1$, l'expression « $\sqrt{-1}$ » n'a pas de sens (sa valuer n'est pas définie).

Exercice. Calculer $\sqrt{64}$, $\sqrt[3]{64}$ et $\sqrt[3]{-64}$.

Voici quelques identités remarquables pour m et n naturels non nuls, a naturel, et x et y entiers, qui sont satisfaites *à la condition que les valeurs des deux membres* (des parties gauche et droite) *soient définies comme nombres entiers* :

(1) $\sqrt[n]{x^a} = \left(\sqrt[n]{x}\right)^a$,

(2) $\sqrt[n]{\sqrt[m]{x}} = \sqrt[nm]{x}$,

(3) $\sqrt[n]{xy} = \sqrt[n]{x}\sqrt[n]{y}$,

(4) $\sqrt[n]{x/y} = \sqrt[n]{x}/\sqrt[n]{y}$,

(5) $\sqrt[n]{1} = 1$, $\sqrt[n]{0} = 0$.

Exercice. Démontrer ces identités.

Observons que $\sqrt{(-1)(-1)} = 1$, alors que la valeur de l'expression « $\sqrt{-1}\sqrt{-1}$ » n'est pas définie (car déjà l'expression « $\sqrt{-1}$ » n'a pas de valeur définie).

II.12. Division euclidienne

Si x et y sont deux entiers avec $y \neq 0$, alors effectuer une *division euclidienne* de x par y veut dire trouver un entier q (le *quotient*) et un entier r (le *reste*) tels que :

(1) $x = yq + r$,

(2) r satisfait une certaine condition précisée d'avance, d'habitude sous forme d'une double inéquation, qui d'habitude assure que le couple (q, r) est unique.

Comme une condition sur le reste qui assure que le couple (q, r) est unique, on peut utiliser, par exemple, une des suivantes :

(1) $0 \leqslant r < |y|$,

(2) $-|y| < r \leqslant 0$,

(3) $0 \leqslant r < y$ ou $y < r \leqslant 0$,

(4) $-|y| < 2r \leqslant |y|$,

(5) $-|y| \leqslant 2r < |y|$.

Exemple. En effectuant la division euclidienne de -100 par -7, on peut, selon la condition souhaitée pour le reste, trouver, par exemple, le quotient 15 et le reste 5, ou le quotient 14 et le reste -2.

II.13. PGCD et PPCM

Les PGCD et les PPCM des nombres entiers sont définies de la même manière que pour les nombres naturels.

Définition. Un nombre entier d est dit un *plus grand commun diviseur* (*PGCD*) de nombres entiers x et y si et seulement si

(1) d est diviseur commun de x et y, et

(2) d est multiple de tout diviseur commun de x et y.

Définition. Un nombre entier m est dit un *plus petit commun multiple* (*PPCM*) de nombres entiers x et y si et seulement si

(1) m est multiple commun de x et y, et

(2) m est diviseur de tout multiple commun de x et y.

Dans le cas des nombres entiers, les PGCD et les PPCM ne sont uniques que lorsque ils sont nuls. En effet, si z est un PGCD de x et y, alors $-z$ l'est aussi, et si z est un PPCM de x et y, alors $-z$ l'est aussi.

Les deux propositions suivantes peuvent être prouvées assez facilement en utilisant l'existence des PGCD et PPCM pour les nombres naturels (ce qui a été prouvé précédemment).

Proposition. *Tous deux nombres entiers ont un unique PGCD positif* (*au sens large*) *et un unique PGCD négatif* (*au sens large*), *et ces deux PGCD sont opposés l'un de l'autre.*

Proposition. *Tous deux nombres entiers ont un unique PPCM positif* (*au sens large*) *et un unique PPCM négatif* (*au sens large*), *et ces deux PPCM sont opposés l'un de l'autre.*

Notation. Pour deux nombres entiers x et y, on va noter « $\operatorname{pgcd}(x, y)$ » l'unique PGCD positif de x et y, et « $\operatorname{ppcm}(x, y)$ » l'unique PPCM positif de x et y.

Observons que $\operatorname{pgcd}(x, y) = \operatorname{pgcd}(|x|, |y|)$, et que $\operatorname{ppcm}(x, y) = \operatorname{ppcm}(|x|, |y|)$.

Le lemme suivant sera utilisé pour justifier un algorithme de calcul du PGCD.

Lemme. *Si x, y, z, q sont quatre nombres entiers tels que $x = y \times q + z$, alors*

(1) *tout diviseur commun de y et z est diviseur de x,*

(2) *tout diviseur commun de x et y est diviseur de z,*

(3) *en particulier, les PGCD de x et y sont les mêmes que les PGCD de y et z.*

Exercice. Prouver ce lemme.

II.14. Algorithme d'Euclide

Pour trouver un PGCD de deux nombres entiers x et y, il suffit de trouver le PGCD naturel des nombres naturels $|x|$ et $|y|$, par exemple par la version de l'*algorithme d'Euclide* pour les nombres naturels.

Autrement, on peut appliquer l'algorithme d'Euclide directement au couple de x et y, avec une condition convenable sur les restes des divisions euclidiennes. Toute condition qui garantie qui la suite des valeurs absolues des restes est strictement décroissante (tant qu'il n'y pas eu du reste 0) convient.

Cependant, on peut réduire le nombres des divisions euclidiennes à effectuer en choisissant une telle condition que la valeur absolue du reste soit toujours inférieure ou égale à la moitié de la valeur absolue du diviseur :

$$\begin{aligned} &r_0 = x, \qquad r_1 = y, \\ &r_0 = r_1 q_2 + r_2, \qquad 2\,|r_2| \leqslant |r_1|\,, \\ &r_1 = r_2 q_3 + r_3, \qquad 2\,|r_3| \leqslant |r_2|\,, \\ &\dots \end{aligned}$$

II.15. Nombres premiers

Tout nombre entier divise 0, mais 0 ne divise que lui-même.

Les nombres ± 1 divisent tous les nombres entiers, mais les seuls nombres entiers qui divisent 1 ou -1 sont 1 et -1.

Ainsi, en ce qui concerne la relation de divisibilité pour les nombres entiers, les nombres 0 et ± 1 sont « les plus singuliers ».

Cependant, certains autres nombres entiers, qui sont dits *premiers*, se distinguent bien par rapport à la relation de divisibilité.

Définition. Un nombre entier a est dit *premier*[4] si et seulement si

(1) a ne divise pas 1, et

(2) les seuls nombres entiers qui divisent a sont ± 1 et $\pm a$.

Observons qu'un nombre entier a est premier si et seulement si $-a$ est premier.

Définition. Les nombres entiers différents de 0 et de ± 1 qui ne sont pas premiers sont dits *composés*.

[4] Si on voulait suivre de près la terminologie de l'algèbre moderne, on devrait appeler ces nombres *irréductibles*, plutôt que premiers, et on devrait appeler *premiers* les nombres p différents de 0 et de ± 1 tels que pour tout produit $a \times b$ qui est divisible par p, a ou b est divisible par p. Cependant, d'après le *lemme d'Euclide*, une telle définition moderne des nombres premiers serait en fait équivalente à la définition donnée ici. Autrement dit, lorsqu'il s'agit des nombres entiers, on peut montrer qu'il n'y a pas de différence entre les éléments irréductibles et les éléments premiers au sens de l'algèbre moderne.

Exemple. Les nombres ± 2, ± 3 et ± 5 sont premiers, alors que les nombres ± 4 et ± 6 sont composés.

Proposition. *Tout nombre entier composé peut être écrit comme un produit de nombres entiers premiers.*

Exercice. Prouver cette proposition.

II.16. Lemme de Bézout

Le lemme suivant est connu sous le nom de *lemme de Bézout*, parmi d'autres.

Lemme (Lemme de Bézout)**.** *Si x et y sont deux entiers et z est leur PGCD, alors il existe deux entiers s et t tels que*

$$z = xs + yt.$$

Exercice. Trouver des nombres entiers s et t tels que $12s + 30t = 6$.

Démonstration du lemme de Bézout. Clairement, il suffit de montrer le lemme pour le cas de x, y, z positifs, donc naturels. Démontrons cela par un raisonnent *par l'absurde* : supposons que cela est faux et en déduisons une absurdité.

Supposons qu'il existe deux nombres entiers positifs x et y tels que leur PGCD positif ne peut pas être écrit comme $xs + yt$ avec s et t entiers. Dans ce cas, il existe un couple de nombres entiers positifs avec cette propriété dont la somme est la plus petite parmi les sommes de tous les couples de nombres entiers positifs avec cette propriété.

Soient donc x et y deux nombres entiers positifs tels que leur PGCD positif ne peut pas être écrit comme $xs+yt$ avec s et t entiers, et qu'en plus la somme $x+y$ est inférieure ou égale à toute somme $u+v$ de nombres entiers positifs u et v dont le PGCD positif ne peut pas être écrit comme $us+vt$ avec s et t entiers. Sans perte de généralité, supposons en plus que $x \geqslant y$. (Sinon on peut échanger les rôles de x et y).

Dans ce cas, $y > 0$, car $\operatorname{pgcd}(x, 0) = x = x \cdot 1 + 0 \cdot 0$. D'où, $(x - y) + y = x < x + y$, et donc $\operatorname{pgcd}(x - y,\ y)$ peut être écrit comme $(x - y)s + yt$ avec s et t entiers (d'après le choix de x et y). Soient donc s et t deux entiers tels que

$$\operatorname{pgcd}(x - y,\ y) = (x - y)s + yt.$$

Or, $\operatorname{pgcd}(x, y) = \operatorname{pgcd}(x - y,\ y)$. Donc,

$$\operatorname{pgcd}(x, y) = (x - y)s + yt = xs + y(t - s).$$

Cela contredit le choix de x et y. □

Utilisons le lemme de Bézout pour en déduire quelques faits utiles.

Lemme. *Si x et y sont deux entiers premiers entre eux, et que z est un multiple commun de x et y, alors xy divise z.*

Démonstration. Soient u et v deux entiers tels que $xu = yv = z$. Soient s et t deux entiers tels que $xs + yt = 1$ (ils existent d'après le lemme de Bézout). Alors

$$z = (xs + yt)z = xsz + ytz = xsyv + ytxu = xy(sv + tu).$$ □

Corollaire. *Si x et y sont deux entiers premiers entre eux, alors xy est un PPCM de x et y.*

Lemme. *Si x et y sont deux entiers, z est un PGCD de x et y, et que w est un multiple commun de x et y, alors xy divise zw.*

Démonstration. Soient u et v deux entiers tels que $xu = yv = w$. Soient s et t deux entiers tels que $xs + yt = z$ (ils existent d'après le lemme de Bézout). Alors

$$zw = (xs + yt)w = xsw + ytw = xsyv + ytxu = xy(sv + tu).$$ □

Corollaire. *Si x et y sont deux entiers, alors*

$$\operatorname{ppcm}(x, y) \operatorname{pgcd}(x, y) = |xy| .$$

Démonstration. Sans perte de généralité, supposons que x et y sont positifs.

Soient u et v deux entiers tels que

$$x = \operatorname{pgcd}(x, y)u \quad \text{et} \quad y = \operatorname{pgcd}(x, y)v.$$

Alors $u \operatorname{pgcd}(x, y)v$ est un multiple commun de x et y. D'où, $\operatorname{ppcm}(x, y) \mid u \operatorname{pgcd}(x, y)v$, et donc

$$\operatorname{ppcm}(x, y) \operatorname{pgcd}(x, y) \mid u \operatorname{pgcd}(x, y)v \operatorname{pgcd}(x, y) = xy.$$

D'après le lemme précédent,

$$xy \mid \operatorname{ppcm}(x, y) \operatorname{pgcd}(x, y).$$

Comme xy et $\operatorname{ppcm}(x, y) \operatorname{pgcd}(x, y)$ sont deux entiers positifs dont chacun divise l'autre, c'est le même. □

Lemme (Lemme d'Euclide généralisé)**.** *Si x et y sont deux entiers et z est un diviseur de xy qui est premier avec x, alors z divise y.*

Démonstration. Soient s et t deux entiers tels que $zs + xt = 1$ (ils existent d'après le lemme de Bézout). Soit w un entier tel que $xy = zw$. Alors

$$y = (zs + xt)y = zsy + xyt = zsy + zwt = z(sy + wt),$$

et donc z divise y. □

II.17. Théorème fondamental de l'arithmétique

À l'aide du *lemme de Bézout*, on peut prouver le *théorème fondamental de l'arithmétique* :

Théorème (Théorème fondamental de l'arithmétique)**.** *Tout nombre naturel composé peut être écrit comme un produit de nombres naturels premiers d'une unique façon, à l'ordre près des facteurs.*

Commençons par les deux lemmes suivants.

Lemme (Lemme d'Euclide)**.** *Si x et y sont deux entiers et p est un diviseur premier de xy, alors p divise x ou p divise y.*

Démonstration. Supposons que p ne divise pas x. Alors p est premier avec x. Soient s et t deux entiers tels que $ps + xt = 1$ (ils existent d'après le lemme de Bézout). Soit q un entier tel que $xy = pq$. Alors

$$y = (ps + xt)y = psy + xyt = psy + pqt = p(sy + qt),$$

et donc p divise y. □

Remarque. Le lemme d'Euclide est un cas particulier du lemme d'Euclide généralisé.

Lemme. *Si $p, q_1, \ldots, q_n$ sont des nombres naturels premiers tels que p divise le produit $q_1 \cdots q_n$, alors il existe un indice i (entre 1 et n) tel que $p = q_i$.*

Démonstration. Posons

$$a_0 = 1, \quad a_1 = q_1, \quad a_2 = q_1q_2, \quad a_3 = q_1q_2q_3, \quad \ldots, \quad a_n = q_1 \cdots q_n.$$

Comme p ne divise pas a_0 mais divise a_n, il existe k entre 1 et n tel que p ne divise pas a_{k-1} mais divise a_k.

Soit k un indice entre 1 et n tel que p ne divise pas a_{k-1} mais divise $a_k = a_{k-1}q_k$. Alors, d'après le lemme précédent, p divise q_k, et donc $p = q_k$. □

Démonstration du théorème fondamental de l'arithmétique. Démontrons ce théorème par un raisonnent *par l'absurde* : supposons qu'il existe un nombre naturel composé qui peut être écrit comme un produit de nombres naturels premiers de deux façons essentiellement différentes, et en déduisons une absurdité.

Supposons qu'il existe un nombre naturel composé qui admet deux écritures comme un produit de nombres naturels premiers de manière qu'un certain nombre premier apparaît comme facteur dans les deux écritures un nombre différent des fois (par exemple, une fois dans une des écritures et deux fois dans l'autre, ou une fois dans une des écritures et pas du tout dans l'autre). Alors, en considérant deux telles écritures et en « supprimant » les facteurs communs dans les deux, on peut trouver un nombre naturel qui admet deux écritures comme un produit de nombres naturels premiers de manière qu'aucun nombre premier n'apparaît comme facteur dans les deux écritures à la fois. Or, cela contredit le lemme précédent. □

Le théorème fondamental de l'arithmétique peut être démontré un peu plus aisément en utilisant la notation suivante :

Notation. Si p est un entier premier et que a est un entier non nul, on va noter « $\nu_p a$ » le plus grand nombre naturel n tel que p^n divise a.

Exemples. $\nu_2 12 = 2$, $\nu_3 12 = 1$, $\nu_5 12 = 0$.

Exercice. Calculer $\nu_3 666$.

Définition. Pour un nombre entier premier p et pour un nombre entier non nul a, le nombre $\nu_p a$ est dit la *valuation p-adique* de a.

Exemple. La valuation triadique (3-adique) de 45 est 2.

Observons que si p et q sont deux nombres entiers premiers, alors

$$\nu_p q = \begin{cases} 1 & \text{si } q = p \text{ ou } q = -p, \\ 0 & \text{sinon.} \end{cases}$$

Proposition. *Si p est un entier premier et a et b sont deux entiers non nuls, alors*

$$\nu_p(ab) = \nu_p a + \nu_p b.$$

Démonstration. Posons $m = \nu_p a$ et $n = \nu_p b$. Soient c et d les entiers tels que $a = p^m c$ et $b = p^n d$. Alors p ne divise ni c, ni d. Donc, d'après le lemme d'Euclide, p ne divise pas cd. Or, $ab = p^{m+n} cd$. D'où, $\nu_p(ab) = m + n = \nu_p a + \nu_p b$. □

Ainsi, si $a_1, \ldots, a_m$ et $b_1, \ldots, b_n$ sont des nombres entiers non nuls tels que

$$a_1 \cdots a_m = b_1 \cdots b_n,$$

alors, pour tout nombre premier p,

$$\nu_p a_1 + \cdots + \nu_p a_m = \nu_p b_1 + \cdots + \nu_p b_n.$$

En particulier, si $a_1, \ldots, a_m$ et $b_1, \ldots, b_n$ sont des nombres naturels premiers tels que

$$a_1 \cdots a_m = b_1 \cdots b_n,$$

alors tout nombre premier apparaît comme facteur dans le premier membre de cette égalité (dans sa parti gauche) autant de fois qu'il apparaît dans son second membre (dans sa partie droite). D'où, $m = n$, et l'expression « $a_1 \cdots a_m$ » ne diffère de l'expression « $b_1 \cdots b_n$ » que par l'ordre des facteurs.

II.18. Congruences

Définition. Soient x, y, z trois entiers. On dit que x est *congru* à y suivant le *module* z, ou *modulo* z, si et seulement si il existe un entier w tel que

$$x = y + zw.$$

Autrement dit, deux entiers x et y sont congrus modulo un entier z si et seulement si z divise $x - y$.

Exercice. (1) Trouver tous les entiers congrus à 5 modulo 0.

(2) Trouver tous les entiers congrus à 5 modulo 1.

(3) Trouver tous les entiers congrus à 5 modulo -1.

Notation. On va écrire « $x \underset{z}{\equiv} y$ » pour dire « x est congru à y modulo z ».

Ainsi, pour tout entier m, on a défini la relation $(\underset{m}{\equiv})$ entre entiers, qui est dite la *relation de congruence modulo m*.

Lorsque la valeur du module m sera précisée dans le contexte, on pourra écrire « $x \equiv y$ » tout court au lieu de « $x \underset{m}{\equiv} y$ », par exemple :

$$2 \equiv 8 \pmod 3.$$

En écriture mathématique contemporaine, il est courant d'abréger « modulo » comme « mod », sans point. Par exemple :

$$2 \equiv 8 \pmod 3.$$

Note étymologique. Le mot « module » vient du latin « *modulus* », qui est la forme diminutive de « *modus* » (qui peut se traduire comme « mesure », « rythme », « borne », « limite », « mode »). Voici le tableau de déclinaison de « *modulus* » en latin :

	Singulier	Pluriel
Nominatif	modulus	modulī
Vocatif	module	modulī
Accusatif	modulum	modulōs
Génitif	modulī	modulōrum
Datif	modulō	modulīs
Ablatif	modulō	modulīs

Proposition. *Les propriétés suivantes sont satisfaites pour tous entiers m, x, y, z :*

(1) *si $x \underset{m}{\equiv} y \underset{m}{\equiv} z$, alors $x \underset{m}{\equiv} z$,*

(2) $x \underset{m}{\equiv} x$,

(3) *si $x \underset{m}{\equiv} y$, alors $y \underset{m}{\equiv} x$.*

Exercice. Prouver cette proposition.

Proposition. *Soient m, x_1, x_2, y_1, y_2 des entiers tels que $x_1 \underset{m}{\equiv} x_2$ et $y_1 \underset{m}{\equiv} y_2$. Alors :*

(1) $x_1 + y_1 \underset{m}{\equiv} x_2 + y_2$, (2) $x_1 - y_1 \underset{m}{\equiv} x_2 - y_2$, (3) $x_1 y_1 \underset{m}{\equiv} x_2 y_2$.

Exercice. Prouver cette proposition.

Lemme. *Si x et y sont deux entiers et que r est le reste d'une division euclidienne de x par y, alors $x \underset{y}{\equiv} r$.*

Exercice. Prouver ce lemme.

Lemme. *Si m, x, y sont des entiers tels que $0 < |x - y| < |m|$, alors $x \underset{m}{\not\equiv} y$.*

Exercice. Prouver ce lemme.

Exercice. Est-ce que le nombre $1^2 + 2^2 + 3^2 + \cdots + 100^2$ est pair ou impair ?

Exercice. Soit $x = 333^{333}$.

(1) Trouver le dernier chiffre de l'écriture binaire de x.

(2) Trouver le dernier chiffre de l'écriture décimale de x.

(3) Trouver le reste de la division euclidienne de x par 7.

Exercice. Soit (Δ) une relation entre des entiers telle que :

(1) si $x \mathrel{\Delta} y \mathrel{\Delta} z$, alors $x \mathrel{\Delta} z$,

(2) $x \mathrel{\Delta} x$,

(3) si $x \mathrel{\Delta} y$, alors $y \mathrel{\Delta} x$,

(4) si $x_1 \mathrel{\Delta} x_2$ et $y_1 \mathrel{\Delta} y_2$, alors $x_1 + y_1 \mathrel{\Delta} x_2 + y_2$, $x_1 - y_1 \mathrel{\Delta} x_2 - y_2$, et $x_1 y_1 \mathrel{\Delta} x_2 y_2$.

Montrer qu'il existe un nombre entier m tel que la relation (Δ) est la congruence modulo m. (Autrement dit : montrer qu'il existe $m \in \mathbf{Z}$ tel que $(\underset{m}{\equiv}) = (\Delta)$.)

Définition. Une *congruence* sur les entiers[5] est une relation (Δ) entre des entiers telle que :

(1) si $x \mathrel{\Delta} y \mathrel{\Delta} z$, alors $x \mathrel{\Delta} z$,

(2) $x \mathrel{\Delta} x$,

(3) si $x \mathrel{\Delta} y$, alors $y \mathrel{\Delta} x$,

(4) si $x_1 \mathrel{\Delta} x_2$ et $y_1 \mathrel{\Delta} y_2$, alors $x_1 + y_1 \mathrel{\Delta} x_2 + y_2$, $x_1 - y_1 \mathrel{\Delta} x_2 - y_2$, et $x_1 y_1 \mathrel{\Delta} x_2 y_2$.

[5] La notion de *congruence* sur les entiers est un cas spécial d'une notion générale de *congruence* sur une *structure algébrique*.

II.19. Classes de congruence, arithmétique modulaire

Définition. Soit m un entier. Définissons les *classes de congruence* d'entiers modulo m ainsi :

(1) à tout entier x, on associe sa *classe de congruence* modulo m, notée « $[x]_m$ »[6] ;

(2) si x et y sont deux entiers, on admet que les *classes de congruence* de x et de y modulo m coïncident si et seulement si x est congru à y modulo m :

$$[x]_m = [y]_m \quad \Leftrightarrow \quad x \underset{m}{\equiv} y.$$

Remarque. Souvent on donne une définition différente des classes de congruence, en les *réalisant* comme des *ensembles* : on dit que la *classe de congruence* de x modulo m est l'ensemble de tous les entiers congrus à x modulo m. En pratique, en tant que l'*arithmétique modulaire* est concernée, cette définition équivaut la nôtre.

Notation. Lorsque la valeur du module m sera précisée dans le contexte, on pourra écrire « $[x]$ » au lieu de « $[x]_m$ ».

Définition. Soit m un entier. Soient α et β deux classes de congruence d'entiers modulo m. On définit la *somme* $\alpha + \beta$, la *difference* $\alpha - \beta$ et le *produit* $\alpha\beta$ ainsi : si x et y sont deux entiers tels que $\alpha = [x]_m$ et $\beta = [y]_m$, alors

(1) $\alpha + \beta = [x]_m + [y]_m \overset{\text{déf}}{=} [x + y]_m$,

(2) $\alpha - \beta = [x]_m - [y]_m \overset{\text{déf}}{=} [x - y]_m$,

(3) $\alpha\beta = [x]_m [y]_m \overset{\text{déf}}{=} [xy]_m$.

Exercice. Montrer que pour tout m entier, les définitions données de l'*addition*, de la *soustraction* et de la *multiplication* des classes de congruence d'entiers modulo m sont correctes et complètes.

Remarque. Il existe une pratique d'écrire « x » tout court à la place de « $[x]_m$ » ou « $[x]$ » lorsque le contexte permet de comprendre qu'il s'agit d'une classe de congruence d'entiers modulo m, plutôt que d'un entier (malgré l'apparence). Ainsi, on peut rencontrer des formules comme celle-là :

« $-2 = 5 \cdot 8 \mod 3$ ».

Cette formule doit alors être lue comme

« $[0]_3 - [2]_3 = [5]_3 \cdot [8]_3$ »,

ou comme « $[0]_3 - [2]_3 = [2]_3 \cdot [2]_3$ », (en simplifiant l'écriture des classes de congruence de 5 et de 8). Selon cette interprétation, dans la formule « $-2 = 5 \cdot 8 \mod 3$ », le numeral « 3 » représente l'entier 3, les numéraux « 2 », « 5 », et « 8 » représentent des classes de congruence d'entiers modulo 3, et les symboles « $-$ » et « $\cdot$ » représentent les opérations de soustraction et de multiplication des classes de congruence d'entiers modulo 3.

[6] La notation « $\bar{x}_m$ » au lieu de « $[x]_m$ » peut aussi être rencontrée.

Proposition. *Soit m un entier et soient α, β, γ des classes de congruence d'entiers modulo m. Alors les identités suivantes sont satisfaites* :

(1) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$,

(2) $\alpha + [0]_m = \alpha = [0]_m + \alpha$,

(3) $\beta + \alpha = \alpha + \beta$,

(4) $(\alpha - \beta) + \beta = \alpha$,

(5) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$,

(6) $\alpha[1]_m = \alpha = [1]_m\alpha$,

(7) $\beta\alpha = \alpha\beta$,

(8) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Exercice. Prouver cette proposition.

Exercice. Soit A l'ensemble des quatre classes de congruence modulo 4 suivantes : $[0]_4, [1]_4, [2]_4, [3]_4$.

(1) Montrer que A contient exactement 4 éléments, c'est-à-dire, que les 4 classes $[0]_4, [1]_4, [2]_4, [3]_4$ sont deux à deux distincts.

(2) Montrer que A contient toutes les classes de congruence d'entiers modulo 4.

(3) Montrer que la somme, la différence, et le produit de deux n'importe quels éléments de A est un élément de A.

(4) Dresser les tables d'addition, de soustraction et de multiplication des éléments de A.

Exercice. Est-il vrai que si α et β sont deux classes de congruence d'entiers modulo un entier m telles que $\alpha \neq [0]_m$ et $\beta \neq [0]_m$, alors $\alpha\beta \neq [0]_m$?