Arithmétique 1

Alexey Muranov

17 avril 2025

Table des matières

I. Nombres naturels

I.1. Qu'est-ce que c'est, un nombre naturel ?

Les *nombres naturels* sont les nombres utilisés à compter et à énumérer des objets. Par exemple : *un*, *deux*, *trois*, *quatre*.

Il y a un cas spécial où on tente de compter des objets alors qu'il n'y en a pas. On peut admettre que dans ce cas le nombre d'objets est *zéro*.

Pour énumérer des objet, on commence d'habitude avec *un*. Cependant, en mathématique et en informatique, on trouve souvent plus pratique de commencer avec *zéro*.

Faut-il donc traiter *zéro* comme un *nombre naturel* ?

En France on admet que *zéro* est un nombre naturel, mais dans certains autres pays les nombres naturels commencent avec *un*. Ici on va suivre la tradition française. Ainsi, on admet que les *nombres naturels* sont : *zéro*, *un*, *deux*, et ainsi de suite à l'infinie.

Dans le *système de numération* romain classique, il n'y a pas de symbole pour le nombre *zéro*, mais à une certaine époque certains auteurs écrivaient « N » pour *zéro*. Le nombre *un* y est noté « I » (la lettre « i » au majuscule, mais « i » minuscule est parfois utilisée aussi).

Dans le système de numération arabe occidental, le nombre *zéro* est noté « 0 » et le nombre *un* est noté « 1 ».

Si on aura besoin de parler de l'*ensemble* des nombres naturels, cet ensemble sera noté « $\mathbf{N}$ ».

I.2. Successeurs et prédécesseurs

Tout nombre naturel possède un unique *successeur* : le nombre naturel suivant. Tout nombre naturel à l'exception de *zéro* est le successeur de son unique *prédécesseur*.

Par exemple, *trois* est le successeur de *deux* et le prédécesseur de *quatre*.

Si a est un nombre naturel, son successeur peut être noté « sa » ou « $s(a)$ » ou « $(s)a$ » (où les parenthèses superflues servent à souligner la différence des rôles de s et de a) ; on lit une telle expression comme « le successeur de a » ou comme « s de a ». Ici on va adopter la notation « sa ».

Ainsi on a défini l'*opération successeur* s qui à chaque nombre naturel associe son successeur. Si on *applique* l'opération s à un nombre naturel a, le résultat sa est le successeur de a.

Par exemple, si 0 est *zéro*, alors $s0$ est *un*, $s(s0)$ est *deux*, $s(s(s0))$ est *trois*, et ainsi de suite.

Voici une propriété importante :

si $sa = sb$, alors $a = b$.

Ainsi, l'opération successeur est « réversible » : on peut déterminer a si on connaît sa.

I.3. Relations d'ordre usuelles

Tous deux nombres naturels a et b peuvent être *comparés* : soit a est *strictement plus grand* que b (et b est *strictement plus petit* que a), soit b est *strictement plus grand* que a (et a est *strictement plus petit* que b), soit ils sont égaux (donc b est a et a est b). En symboles, on exprime cela ainsi : soit $a > b$ (et $b < a$), soit $b > a$ (et $a < b$), soit $a = b$.

Au lieu d'écrire « $a < b$ ou $a = b$ », on peut écrire « $a \leqslant b$ », et au lieu d'écrire « $a > b$ ou $a = b$ », on peut écrire « $a \geqslant b$ ».

Le sens de ces relations est le suivant : si a est le nombre d'objets dans une collection finie A (dans un ensemble fini A) et b est le nombre d'objets dans une partie B de A, alors $a \geqslant b$. Si en plus il existe un objet dans A qui n'est pas dans B, alors $a > b$.

Voici les trois propriétés de la relation $(<)$ les plus importantes :

(1) si $a < b$ et $b < c$, alors $a < c$,

(2) si $a < b$, alors $a \neq b$,

(3) si $a \neq b$, alors $a < b$ ou $b < a$.

Ajoutons à cette liste une quatrième propriété qui fait lien avec l'opération successeur :

(4) $a < sa$.

I.4. Addition

Si a est le nombre d'objet dans une collection finie (dans un ensemble fini), b est le nombre d'objets dans une deuxième collection finie (dans un deuxième ensemble fini), et que les deux collections n'ont pas d'objets en commun (on dit dans ce cas qu'elles sont *disjointes*), alors si on réunit les deux collections, le nombre d'objets dans la collection réunie est *a plus b*, autrement dit la *somme* de a et b. La somme de a et b ne dépend que de a et de b (la nature des objets et les collections en question sont sans importance).

Par exemple, on peut observer que la somme de *deux* et *trois* est *cinq* en utilisant cinq n'importe quels objets, par exemple cinq pommes, en séparant deux objets des trois autres.

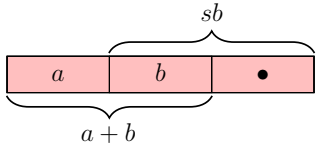
Si a et b sont deux nombres naturels, on note « $a + b$ » leur somme.

Ainsi on a défini l'*opération d'addition* $(+)$ qui à deux nombres naturels associe leur somme.

L'addition $(+)$ de nombres naturels peut aussi être définie par les deux règles suivantes, en utilisant uniquement l'opération successeur s et le nombre *zéro* 0 :

(1) $a + 0 = a$, (2) $a + sb = s(a + b)$.

Le schéma suivant montre que la règle (2) est en accord avec la notion de l'addition introduite précédemment :



Exercice. En utilisant uniquement les deux règles données ci-dessus, montrer que

$$s(s0) + s(s(s0)) = s(s(s(s(s0)))).$$

Voici les trois identités les plus importantes satisfaites par l'opération d'addition (pour les nombres naturels) :

(1) $a + (b + c) = (a + b) + c$,

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

(3) $b + a = a + b$.

Exercice. Démontrer ces identités (au moins d'une manière informelle).

Voici une propriété importante :

si $a + c = b + c$, alors $a = b$.

Ainsi, pour tout nombre naturel a, l'opération d'addition de a (à un autre nombre naturel) est « réversible » : on peut déterminer b si on connaît $b + a$ et a.

Cette dernière propriété s'écrit autrement ainsi :

si $a \neq b$, alors $a + c \neq b + c$.

On peut observer une propriété plus précise :

si $a < b$, alors $a + c < b + c$.

Définition des relations d'ordre à l'aide de l'addition

L'opération d'addition $(+)$ peut servir à définir les relations $(\leqslant)$ et $(<)$ par les règles suivantes :

(1) $a \leqslant b$ si et seulement si il existe c tel que $b = a + c$,

(2) $a < b$ si et seulement si il existe c différent de *zéro* tel que $b = a + c$.

Attention : ces règles ne concernent que les nombres naturels.

I.5. Soustraction

La définition de l'opération de *soustraction* repose sur la propriété suivante des nombres naturels :

si $b + a = c + a$, alors $b = c$.

Rappelons nous aussi que

$a \leqslant b$ si et seulement si il existe c tel que $c + a = b$.

Soient a et b deux nombre naturel. On peut tenter de chercher un nombre naturel c tel que $c + a = b$. Si $a > b$, on n'en trouvera aucun, et si $a \leqslant b$, on en trouvera un, et un seul. Dans le second cas, l'unique nombre c tel que $c + a = b$ est noté « $b - a$ » et est dit b *moins* a, ou encore la *différence* de b et a. Si $a > b$, alors la valeur de « $b - a$ », en tant qu'un nombre naturel, n'est pas définie. (Mais on pourra définir la valeur de « $b - a$ » comme un *entier relatif*.)

Par exemple, *trois* moins *un* est *deux*, mais aucun nombre naturel n'est *zéro* moins *un*.

Ainsi on a défini l'*opération de soustraction* $(-)$ qui à deux nombres naturels associe leur différence, tant que leur différence est définie.

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

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

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

(1) $(a + b) - b = a$,

(2) $(a - b) + b = a$ si $b \leqslant a$,

(3) la valeur de « $a - b$ » n'est définie (comme un nombre naturel) que si $b \leqslant a$.

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.[1]

Voici quelques identités remarquables satisfaites par l'opération de soustraction (pour les nombres naturels) :

(1) $a + (b - c) = (a + b) - c$ si $c \leqslant b$,

[1] Supposons que l'opération $(-)$ est définie de telle façon que $(a + b) - b = a$ pour tous les nombres naturels a et b. Soient a et b deux nombres naturels arbitraires mais tels que $b \leqslant a$. Alors il existe un nombre naturel c tel que $a = c + b$. Or, si $a = c + b$, alors $(a - b) + b = ((c + b) - b) + b = c + b = a$, car $(c + b) - b = c$.
Supposons maintenant que l'opération $(-)$ est définie de telle façon que $(a - b) + b = a$ pour tous les nombres naturels a et b tels que $b \leqslant a$. Soient a et b deux nombres naturels arbitraires et posons $c = a + b$. Alors $\underbrace{((a + b) - b)} + b = (c - b) + b = c = \underline{a} + b$, et donc $(a + b) - b = a$.

(2) $a-(b+c)=(a-c)-b$ si $b+c\leqslant a$,

(3) $a-(b-c)=(a+c)-b$ si $c\leqslant b\leqslant a+c$,

(4) $(a-b)+(b-c)=a-c$ si $c\leqslant b\leqslant a$,

(5) $(a+c)-(b+c)=a-b$ si $b\leqslant a$,

(6) $(a-b)+c=(a+c)-b$ si $b\leqslant a$,

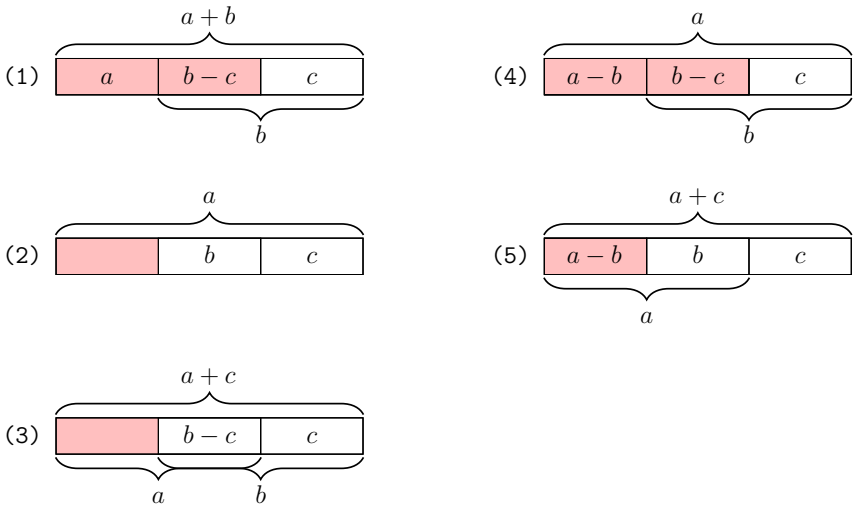
(7) $(a-b)-c=(a-c)-b$ si $b+c\leqslant a$,

(8) $a-(a-b)=b$ si $b\leqslant a$,

(9) $a-0=a$,

(10) $a-a=0$.

Les schémas suivants peuvent être éclairants :



Exercice. Démontrer ces identités (au moins d'une manière informelle).

Exercice. Déduire ces identités algébriquement à partir des propriétés algébriques de l'addition présentées précédemment.

I.6. Systèmes de numération

Pour pouvoir utiliser des nombres naturels individuels, il faut pouvoir les appeler et les écrire. Or, il y a une infinité des nombres naturels, donc on ne peut pas les considérer un par un et donner à chacun un nom et un symbole.

En principe, il suffit d'avoir un symbole pour *zéro*, par exemple « ∗ », et un symbol pour l'opération successeur, par exemple « s », pour pouvoir écrire un n'importe quel nombre naturel : $s*$ est *un*, $s(s*)$ est *deux*, $s(s(s*))$ est *trois*, et ainsi de suite.

On peut aussi écrire un n'importe quel nombre naturel non nul en utilisant un symbole pour le nombre *un* et un symbole pour l'opération d'addition. Par exemple, si « I » est un symbole pour *un*, et « + » est un symbole pour l'addition, alors I est *un*, I + I est *deux*, (I + I) + I est *trois*, et ainsi de suite.

Cependant, écrire les nombres naturels comme des longues expressions arithmétiques n'est pas toujours pratique. Ainsi, souvent on préfère d'utiliser un *systèmes de numération* plus ou moins « compact » pour « nommer » les nombres.

Le tableau I.1 contient quelques exemples de *systèmes de numération* qu'on pourrait envisager, et qui sont en effet utilisés.

	zéro	un	deux	trois	quatre	cinq	six	dix	onze	douze	seize	mille
(a)		|	||	|||	||||	|||||	||||||	||||||||||	|||||||||||	||||||||||||	||||||||||||||||	|···|
(b)		|	||	|||	||||	𝍸	𝍸|	𝍸𝍸	𝍸𝍸|	𝍸𝍸||	𝍸𝍸|||	𝍸𝍸||||	𝍸 ··· 𝍸
(c)		I	II	III	IV	V	VI	X	XI	XII	XVI	M
(d)	0	1	10	11	100	101	110	1010	1011	1100	10000	1111101000
(e)	0	1	2	10	11	12	20	101	102	110	121	1101001
(f)	0	1	2	3	4	5	6	10	11	12	16	1000
(g)	0	1	2	3	4	5	6	A	B	C	10	3E8

Tab. I.1. : Exemples de systèmes de numération

Le système (c) est le système romain classique. Le système (f) est le système arabe occidental.

Les systèmes (d), (e), (f) et (g) sont tous construits sur le même principe. La seule différence entre ces systèmes est le nombre des *chiffres* utilisés :

- le système (d) utilise les deux chiffres « 0 » et « 1 »,
- le système (e) utilise les trois chiffres « 0 », « 1 » et « 2 »,
- le système (f) utilise les dix chiffres « 0 », « 1 », « 2 », « 3 », « 4 », « 5 », « 6 », « 7 », « 8 », « 9 »,
- le système (g) utilise seize chiffres : les dix de « 0 » à « 9 », et encore les six de « A » à « F » (ou de « a » à « f »).

Ces systèmes font partie des systèmes de numération dits *positionnels*, car la « valeur » de chaque chiffre qui apparaît dans l'écriture d'un nombre dépend de la *position* de cette chiffre dans l'écriture. Ces systèmes parfois sont dits *n-aires*, où n est le nombre des chiffres utilisés. Pour décrire ces systèmes, on utilise aussi des adjectifs d'origine

latine, ou grecque, ou latin et grecque, comme : *binaire*, *ternaire*, *quaternaire*. Ainsi, le système `(d)` est dit *binaire* (ou *deux-aire*), le système `(e)` est dit *ternaire* (ou *trois-aire*), le système `(f)` est dit *décimal* (ou *dix-aire*), et le système `(g)` est dit *hexadécimal* (ou *seize-aire*).

Pour un système positionnel n-aire, le nombre n (le nombre des chiffre) est dit la *base* du système. Ainsi, la base du système `(d)` est *deux*, la base du système `(e)` est *trois*, la base du système `(f)` est *dix*, et la base du système `(g)` est *seize*.

Dans ce cours, la plupart du temps on va utiliser le système arabe occidental (le système `(f)`). Ainsi, par défaut, « 10 » veut dire *dix*, « 100 » veut dire *cent*, et ainsi de suite.

Si on souhaite utiliser un système positionnel n-aire avec n différent de *dix* sans avertissement, on peut convenir à préciser la base en indice, écrit en système décimal. Ainsi, « 10_2 » veut dire *deux*, « 100_3 » veut dire *neuf*, et « 34_5 » veut dire *dix-neuf* :

$$34_5 = 30_5 + 4_5 = 10_5 + 10_5 + 10_5 + 4_5 = 5 + 5 + 5 + 4 = 10 + 9 = 19.$$

En fait, rien n'empêche d'écrire la base en n'importe quel système. Par exemple, comme « 12_3 » veut dire *cinq*, « 34_{12_3} » veut dire *dix-neuf*.

Exercice. Écrire le nombre *vingt-cinq* en binaire, puis en ternaire, puis en décimal, puis en hexadécimal (les systèmes `(d)`, `(e)`, `(f)` et `(g)`).

Exercice. Dresser les tables d'addition pour les systèmes binaire et quinaire (les bases *deux* et *cinq*). Pour chaque système, toutes les valeurs dans sa table doivent être écrites en ce système.

I.7. Multiplication

Étant données a collectons d'objets, où chaque collection contient b objets et où aucunes deux d'entre elles n'ont d'objets en commun (toutes deux collections sont disjointes), le nombre d'objets que ces a collections contiennent ensemble est a *fois* b :

$$\underbrace{b + b + \cdots + b}_{a \text{ fois}}.$$

Cette définition peut paraître inadaptée si a est *un* ou *zéro*, mais il suffit de préciser que *une fois* b est b et que *zéro fois* b est *zéro*. On peut aussi définir a *fois* b comme

$$0 \underbrace{+ b + b + \cdots + b}_{a \text{ fois}}.$$

Le nombre a fois b est aussi dit b *multiplié* par a.

Adoptons les notations « $a \ltimes b$ » et « $b \rtimes a$ » pour écrire a fois b, quand a et b sont deux nombres naturels. Ainsi, pour a et b naturels :

$$a \ltimes b \overset{\text{déf}}{=} 0 \underbrace{+ b + b + \cdots + b}_{a \text{ fois}},$$

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

Exercice. Calculer $2 \ltimes 2$, $2 \rtimes 2$, $2 \ltimes 3$, $2 \rtimes 3$, $2 \ltimes (3 \ltimes 4)$, $(2 \ltimes 3) \ltimes 4$.

Exercice. Supposons qu'il y a a conteneurs sur une plate-forme, que chaque conteneur contient b cartons, et que chaque carton contient c canettes.

`(1)` Montrer que le nombre total des canettes sur la plate-forme est $a \ltimes (b \ltimes c)$.

`(2)` Montrer que le nombre total des canettes sur la plate-forme est $(a \ltimes b) \ltimes c$.

Exercice. Démontrer (au moins d'une manière informelle) que pour tous nombres naturels a, b et c, $a \rtimes (b \rtimes c) = (a \rtimes b) \rtimes c$.

Évidemment, pour tous a et b naturels, $b \rtimes a = a \ltimes b$ (par définition). Cependant, on peut être surpris de remarquer que

$$4 \ltimes 3 = \underbrace{3 + 3 + 3 + 3}_{4 \text{ fois}} = 12 = \underbrace{4 + 4 + 4}_{3 \text{ fois}} = 3 \ltimes 4.$$

Est-ce une coïncidence ?

Exercice. Déterminer s'il existe deux nombres naturels a et b plus petits que 5 tels que $b \ltimes a \neq a \ltimes b$.

Exercice. Démontrer (au moins d'une manière informelle) que pour tous nombres naturels a et b, $b \ltimes a = a \ltimes b$.

On peut montrer que pour tous nombres naturels a et b, b fois a est le même nombre que a fois b : $b \ltimes a = a \ltimes b$, ou, écrit autrement,

$$a \rtimes b = a \ltimes b.$$

Le *produit* de nombres naturels a et b est défini, indifféremment, comme a fois b ou comme b fois a, et est traditionnellement noté « $a \times b$ », ou « $a \cdot b$ », ou tout simplement « ab ».

Ainsi on a défini l'*opération de multiplication* ($\times$) (aussi notée « $(\cdot)$ ») qui à deux nombres naturels a et b associe leur produit $ab = a \cdot b = a \times b = a \ltimes b = a \rtimes b$.

Exercice. `(1)` Calculer le produit $a \times b$ pour tous les nombres naturels a et b de 1 à 9 (dresser la table de multiplication).

`(2)` Dresser les tables de multiplication pour les bases 2 et 5. Pour chaque base, toutes les valeurs dans sa table doivent être écrites en cette base.

La multiplication ($\times$) de nombres naturels peut aussi être définie par les deux règles suivantes, en utilisant uniquement l'opération d'addition ($+$), l'opération successeur s, et le nombre *zéro* 0 :

`(1)` $a \times 0 = 0$, `(2)` $a \times sb = a \times b + a$.

Voici les six identités les plus importantes satisfaites par l'opération de multiplication (pour les nombres naturels) :

(1) $a \times (b \times c) = (a \times b) \times c$,

(2) $a \times 1 = a = 1 \times a$,

(3) $b \times a = a \times b$,

(4) $a \times (b + c) = a \times b + a \times c$,

(5) $a \times (b - c) = a \times b - a \times c$ si $c \leqslant b$,

(6) $a \times 0 = 0$.

Exercice. Démontrer ces identités (au moins d'une manière informelle).

Voici deux propriétés importantes :

(1) si $a \neq 0$ et $b \neq 0$, alors $a \times b \neq 0$,

(2) si $a \times c = b \times c$ et que $c \neq 0$, alors $a = b$.

Ainsi, pour tout nombre naturel $a \neq 0$, l'opération de multiplication par a (d'un autre nombre naturel) est « réversible » : on peut déterminer b si on connaît $b \times a$ et a.

La dernière propriété s'écrit autrement ainsi :

si $a \neq b$ et $c \neq 0$, alors $a \times c \neq b \times c$.

On peut observer une propriété plus précise :

si $a < b$ et $c > 0$, alors $a \times c < b \times c$.

I.8. Divisibilité

On dit qu'un nombre naturel a *divise* un nombre naturel b si et seulement si il existe un nombre naturel c tel que $b = a \times c$.

Par exemple, 2, 3 et 4 divisent 12, mais 5 ne le divise pas. Tout nombre naturel divise 0. Le nombre 0 ne divise que lui-même. Le nombre 1 divise tout.

On utilise la notation « $a \mid b$ » pour dire « a divise b », par exemple : $3 \mid 12$, $5 \nmid 12$, $5 \mid 0$, $0 \mid 0$, $0 \nmid 5$, $1 \mid 5$.

Ainsi on a défini la *relation de divisibilité* ($\mid$) entre nombres naturels.

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

(1) a divise b,

(2) b se factorise par a,

(3) a est diviseur de b,

(4) b est multiple de a.

Par exemple, 3 est diviseur de 12, et 12 est multiple de 3.

Les nombres naturels qui sont multiples de 2 sont dits *pairs*, et les autres sont dits *impairs*.

Proposition. *Si un nombre naturel a divise un nombre naturel $b \neq 0$, alors $1 \leqslant a \leqslant b$.*

Exercice. Prouver cette proposition.

Voici les trois propriétés les plus importantes de la relation de divisibilité ($\mid$) de nombres naturels :

(1) si $a \mid b$ et $b \mid c$, alors $a \mid c$,

(2) $a \mid a$,

(3) si $a \mid b$ et $b \mid a$, alors $a = b$.

Exercice. Démontrer les trois propriétés.

Remarque. Si on définit la relation de divisibilité pour les *entiers relatifs* de la manière analogique, la propriété (3) pour la divisibilité des entiers relatifs ne sera pas satisfaite.

Remarque. Les relations d'ordre ($\leqslant$) et ($\geqslant$) sur les nombres naturels (ainsi que sur les entiers relatifs, ou sur les réels) satisfont les mêmes trois propriétés que celles données ci-dessus pour la divisibilité des nombres naturels.

Définition. Un nombre naturel d est dit *diviseur commun* (ou *commun diviseur*) de plusieurs nombres naturels donnés si et seulement si d est diviseur de chacun de ces nombres.

Exemple. Les nombres naturels 1, 2, 6 sont diviseurs communs de 12 et 18. Les nombres naturels 10 et 15 sont diviseurs communs de 0, 30 et 60.

Définition. Deux nombres naturels sont dits *premiers entre eux* si et seulement si le nombre 1 est leur seul diviseur commun (naturel). Au lieu de dire que a et b sont premiers entre eux, on peut aussi dire que a est *premier avec* b.

Exemple. Les nombres naturels 10 et 21 sont premiers entre eux, mais 10 et 15 ne le sont pas (5 est un diviseur commun de 10 et 15).

Définition. Un nombre naturel m est dit *multiple commun* (ou *commun multiple*) de plusieurs nombres naturels donnés si et seulement si m est multiple de chacun de ces nombres.

Exemple. Les nombres naturels 0, 30, 60 sont multiples communs de 10 et 15. Les nombres naturels 12 et 18 sont multiples communs de 1, 2 et 6.

Proposition. *Soient a, b, c trois nombres naturels tels que c divise a et b. Alors c divise $a + b$. Si, en plus, $a \geqslant b$, alors c divise $a - b$.*

Exercice. Prouver cette proposition.

Exercice. (1) Montrer qu'un nombre naturel est multiple de 3 si et seulement si la somme des chiffres de son écriture décimale est multiple de 3.

(2) Prouver l'énoncé analogique pour la divisibilité par 9.

(3) Montrer qu'un nombre naturel est multiple de 5 si et seulement si la somme des chiffres de son écriture hexadécimale est multiple de 5.

I.9. Division

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

si $b \times a = c \times a$ et $a \neq 0$, alors $b = c$.

Soient a et b deux nombres naturels. On peut tenter de chercher un nombre naturel c tel que $c \times a = b$. Si $a \nmid b$, il n'y en a pas. Si $a = b = 0$, alors tout nombre naturel c convient. Si $a \neq 0$ et que $a \mid b$, alors il y a un et un seul nombre naturel c tel que $a \times c = c \times a = b$. Dans ce dernier cas, l'unique nombre c tel que $c \times a = b$ est dit le *quotient* de b par a et est noté « $b \div a$ », ou « $b : a$ », ou « b/a », ou « $a\backslash b$ », ou « $\frac{b}{a}$ ». Dans les autres cas, aucun nombre naturel n'est dit « quotient de b par a ». (Mais on pourra définir le quotient de b par a comme un nombre *rationnel* tant que $a \neq 0$.)

Par exemple, $12 \div 3 = 4$, mais on n'a pas défini la valeur de l'expression « $12 \div 5$ », ni la valeur de l'expression « $12 \div 0$ », ni la valeur de l'expression « $0 \div 0$ », comme un nombre naturel.

Ainsi on a défini l'*opération de division* ($\div$) (aussi notée « $(/)$ » ou parfois « $(:)$ ») qui à deux nombres naturels associe leur quotient, tant que leur quotient est défini.

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

$$b \div a = c \quad \Leftrightarrow \quad \begin{cases} a \neq 0 \\ b = c \times a \end{cases}.$$

L'opération de division ($\div$) de nombres naturels peut aussi être définie par les trois propriétés suivantes, à la condition que l'opération de multiplication ($\times$) est déjà définie :

(1) $(a \times b) \div b = a$ si $b \neq 0$,

(2) $(a \div b) \times b = a$ si $b \mid a$ et $b \neq 0$,

(3) la valeur de « $a \div b$ » n'est définie (comme un nombre naturel) que si $b \mid a$ et $b \neq 0$.

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.[2]

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

(1) $a \times (b \div c) = (a \times b) \div c$ si $c \mid b$ et $c \neq 0$,

(2) $a \div (b \times c) = (a \div c) \div b$ si $b \times c \mid a$ et $b \times c \neq 0$,

(3) $a \div (b \div c) = (a \times c) \div b$ si $c \mid b \mid a \times c$ et $b \neq 0$,

(4) $(a \div b) \times (b \div c) = a \div c$ si $c \mid b \mid a$ et $b \neq 0$,

(5) $(a \times c) \div (b \times c) = a \div b$ si $b \mid a$ et $b \times c \neq 0$,

(6) $(a \div b) \times c = (a \times c) \div b$ si $b \mid a$ et $b \neq 0$,

(7) $(a \div b) \div c = (a \div c) \div b$ si $b \times c \mid a$ et $b \times c \neq 0$,

(8) $a \div (a \div b) = b$ si $b \mid a$ et $a \neq 0$,

(9) $a \div 1 = a$,

(10) $a \div a = 1$ si $a \neq 0$,

(11) $(a + b) \div c = a \div c + b \div c$ si $c \mid a$, $c \mid b$ et $c \neq 0$,

(12) $(a - b) \div c = a \div c - b \div c$ si $c \mid a$, $c \mid b$, $c \neq 0$ et $b \leqslant a$,

(13) $0 \div a = 0$ si $a \neq 0$.

Exercice. Démontrer ces identités (au moins d'une manière informelle).

Exercice. Déduire ces identités algébriquement à partir des propriétés algébriques de la multiplication présentées précédemment.

[2] Supposons que l'opération ($\div$) est définie de telle façon que $(a \times b) \div b = a$ pour tous les nombres naturels a et b tels que $b \neq 0$. Soient a et b deux nombres naturels arbitraires mais tels que $b \mid a$ et $b \neq 0$. Alors il existe un nombre naturel c tel que $a = c \times b$. Or, si $a = c \times b$, alors $(a \div b) \times b = ((c \times b) \div b) \times b = c \times b = a$, car $(c \times b) \div b = c$.
Supposons maintenant que l'opération ($\div$) est définie de telle façon que $(a \div b) \times b = a$ pour tous les nombres naturels a et b tels que $b \mid a$ et $b \neq 0$. Soient a et b deux nombres naturels arbitraires et posons $c = a \times b$. Alors $\underbrace{((a \times b) \div b)} \times b = (c \div b) \times b = c = \underbrace{a} \times b$, et donc $(a \times b) \div b = a$.

I.10. Exponentiation, puissances

Si a et b sont deux nombres naturels, alors la b-ième *puissance* de a, ou a *élevé à la* b*-ième puissance*, ou a *puissance* b, est le nombre noté « a^b » et défini ainsi :

$$a^b \overset{\text{déf}}{=} 1 \underbrace{\times a \times a \times \cdots \times a}_{b \text{ fois}}.$$

Par exemple : $a^0 = 1$, $a^1 = a$, $a^2 = a \times a$, $a^3 = a \times a \times a$.

Dans une expression de la forme « a^b », la valeur de « a » est dit la *base*, et la valeur de « b » est dit l'*exposant*.

Le nombre a^b est aussi dit a *exposant* b, ainsi que l'*exponentielle* de b en *base* a.

Ainsi on a défini l'*opération puissance*, ou l'*opération d'exponentiation*, qui à deux nombres naturels a et b associe le nombre a^b (la b-ième puissance de a, l'exponentielle de b en base a).

Si a est un nombre naturel, alors le *carré* de a, ou a *au carré*, est le nombre $a^2 = a \times a$ (a puissance 2), et le *cube* de a, ou a *au cube*, est le nombre $a^3 = a \times a \times a$ (a puissance 3).

L'exponentiation de nombres naturels peut aussi être définie par les deux règles suivantes, en utilisant uniquement l'opération de multiplication, l'opération successeur s, et les nombres *zéro* 0 et *un* 1 :

(1) $a^0 = 1$, (2) $a^{sb} = a^b \times a$.

Remarque. Il n'y a pas de consensus général sur le sens de « 0^0 ». D'après la définition donnée ici, $0^0 = 1$. Cependant, en *analyse mathématique*, parfois on décide que l'expression « 0^0 » n'ait pas de sens ou que sa valeur ne soit pas définie (comme pour « $0 \div 0$ »).

Exercice. Supposons qu'on a n jours pour réviser m matières, et qu'on veut chaque jour réviser une et une seule matière. En revanche, on peut passer plusieurs jours à réviser une même matière, on peut alterner entre différentes matières, et ne pas réviser certaines parmi elles. Il reste à décider quel jour on revise quelle matière. Montrer qu'on a exactement m^n possibilités.

Voici quelques identités remarquables satisfaites par l'opération d'exponentiation (pour les nombres naturels) :

(1) $a^{b \times c} = (a^b)^c$,

(2) $a^1 = a$,

(3) $a^{b+c} = a^b \times a^c$,

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

(5) $a^0 = 1$,

(6) $(a \times b)^c = a^c \times b^c$,

(7) $(a \div b)^c = a^c \div b^c$ si $b \neq 0$ et $b \mid a$,

(8) $1^c = 1$.

Exercice. Démontrer ces identités (au moins d'une manière informelle).

Voici deux propriétés importantes :

(1) si $a^c = b^c$ et que $c \neq 0$, alors $a = b$,

(2) si $c^a = c^b$ et que $c \neq 0$ et $c \neq 1$, alors $a = b$.

Ainsi,

(1) pour tout nombre naturel $a \neq 0$, l'opération qui à tout nombre naturel b associe b^a est « réversible », et

(2) pour tout nombre naturel $a > 1$, l'opération qui à tout nombre naturel b associe a^b est « réversible ».

Ces deux propriétés s'écrivent autrement ainsi :

(1) si $a \neq b$ et $c \neq 0$, alors $a^c \neq b^c$,

(2) si $a \neq b$, $c \neq 0$ et $c \neq 1$, alors $c^a \neq c^b$.

On peut observer deux propriétés plus précises :

(1) si $a < b$ et $c > 0$, alors $a^c < b^c$,

(2) si $a < b$ et $c > 1$, alors $c^a < c^b$.

I.11. Exponentiations itérées, notation de Knuth

Donald Knuth a proposé d'utiliser une notation avec des flèches pour l'opération d'exponentiation, ainsi que pour les *exponentiations (ré-)itérées*.[3]

Avec la notation de Knuth, « $a \uparrow b$ » veut dire a^b :

$$a \uparrow b \overset{\text{déf}}{=} a^b = \underbrace{a \times (\cdots \times (a \times}_{b \text{ fois}} 1) \cdots).$$

Les opérations ($\uparrow\uparrow$), ($\uparrow\uparrow\uparrow$), et ainsi de suite, sont définies par récurrence :

$$a \uparrow\uparrow b \overset{\text{déf}}{=} \underbrace{a \uparrow (\cdots \uparrow (a \uparrow}_{b \text{ fois}} 1) \cdots),$$
$$a \uparrow\uparrow\uparrow b \overset{\text{déf}}{=} \underbrace{a \uparrow\uparrow (\cdots \uparrow\uparrow (a \uparrow\uparrow}_{b \text{ fois}} 1) \cdots),$$

et ainsi de suite.

[3] Le terme « puissances itérées » à la place d'« exponentiations itérées » est courant. Cependant, ce n'est pas une *fonction puissance* qui est itérée dans « $a \uparrow\uparrow b$ », mais une *fonction exponentielle*. On pourrait dire que pour calculer $2 \uparrow 2$ on effectue une exponentiation, pour calculer $2 \uparrow\uparrow 2$ on effectue une exponentiation itérée, pour calculer $2 \uparrow\uparrow\uparrow 2$ on effectue une exponentiation itérée itérée, et ainsi de suite.

Par example :

$$\begin{aligned}
&2 \uparrow 3 = 2 \times (2 \times (2 \times 1)) = 2 \times 2 \times 2 = 8,\\
&3 \uparrow 2 = 3 \times (3 \times 1) = 3 \times 3 = 9,\\
&2 \uparrow\uparrow 3 = 2 \uparrow (2 \uparrow (2 \uparrow 1)) = 2 \uparrow (2 \uparrow 2) = 2 \uparrow 4 = 16,\\
&3 \uparrow\uparrow 2 = 3 \uparrow (3 \uparrow 1) = 3 \uparrow 3 = 27.
\end{aligned}$$

Les opérations $(\uparrow)$, $(\uparrow\uparrow)$, $(\uparrow\uparrow\uparrow)$, et ainsi de suite, peuvent aussi être définies à l'aide de l'opération successeur s :

$$\begin{aligned}
a \uparrow 0 &= 1, & a \uparrow sb &= a \times (a \uparrow b),\\
a \uparrow\uparrow 0 &= 1, & a \uparrow\uparrow sb &= a \uparrow (a \uparrow\uparrow b),\\
a \uparrow\uparrow\uparrow 0 &= 1, & a \uparrow\uparrow\uparrow sb &= a \uparrow\uparrow (a \uparrow\uparrow\uparrow b),\\
&\dots
\end{aligned}$$

Exercice. Calculer $2 \uparrow\uparrow\uparrow 3$ et $3 \uparrow\uparrow\uparrow 2$.

Observons que pour tout nombre naturel a,

$$a = a + 0 = a \times 1 = a \uparrow 1 = a \uparrow\uparrow 1 = a \uparrow\uparrow\uparrow 1 = \cdots .$$

Une autre observation curieuse :

$$4 = 2 + 2 = 2 \times 2 = 2 \uparrow 2 = 2 \uparrow\uparrow 2 = 2 \uparrow\uparrow\uparrow 2 = \cdots .$$

I.12. Factorielle

Considérons l'opération qui à tout nombre naturel a associe un nombre naturel noté « $a!$ », définie par les deux règles suivantes :

(1) $0! \overset{\text{déf}}{=} 1$, (2) $(sa)! \overset{\text{déf}}{=} a! \times sa$.

Si a est un nombre naturel, alors le nombre $a!$ défini ci-dessus est dit la *factorielle* de a, ou *a-factorielle*.

Exemple. La factorielle de 1 est 1, la factorielle de 2 est 2, la factorielle de 3 est 6.

Exercice. Calculer 4!, 5!, 6!.

Exercice. Supposons qu'on a n jours pour réviser n matières, et qu'on veut réviser chaque matière en un jour, et qu'on veut chaque jour ne reviser qu'une seule matière. Il reste à décider quel jour on revise quelle matière. Montrer qu'on a exactement $n!$ possibilités.

Exercice. Combien de semaines y a-t-il dans 10! secondes ?

I.13. Division entière (division euclidienne)

Proposition. *Soient a et b deux nombres naturels tels que $b \neq 0$. Alors il existe un unique couple de nombres naturels q et r tel que* :

$$a = b \times q + r \quad et \quad r < b.$$

Exercice. Prouver cette proposition.

Définition. Si a, b, q, r sont quatre nombres naturels tels que $b \neq 0$ et que

$$a = b \times q + r \quad \text{et} \quad r < b,$$

alors le nombre q est dit le *quotient* de la *division entière* de a par b, et le nombre r est dit le *reste* de la division entière de a par b. On dit aussi *division euclidienne* au lieu de *division entière*.

Exemple. Le quotient et le reste de la division entière de 100 par 7 sont 14 et 2, car $100 = 7 \times 14 + 2$ et $2 < 7$.

Le système de numération décimal usuel, ainsi que les systèmes de numération analogues de toutes les autres bases, permet d'effectuer la division entière par un algorithme plus ou moins efficace. Par exemple, trouvons le quotient et le reste de la division entière de 2222 par 33. Commençons par observer que $33 \times 100 = 3300 > 2222$. Ensuite, effectuons la division entière de 2222 par $33 \times 10 = 330$:

$$\begin{aligned}
2222 &= 330 \times 1 + 1892\\
&= 330 \times 2 + 1562\\
&= 330 \times 3 + 1232\\
&= 330 \times 4 + 902\\
&= 330 \times 5 + 572\\
&= 330 \times 6 + 242 \qquad (330 \times 6 = 1980).
\end{aligned}$$

Donc, le quotient de la division entière de 2222 par 330 est 6, et le reste est 242. Maintenant, effectuons la division entière de 242 par 33 :

$$\begin{aligned}
242 &= 33 \times 1 + 209\\
&= 33 \times 2 + 176\\
&= 33 \times 3 + 143\\
&= 33 \times 4 + 110\\
&= 33 \times 5 + 77\\
&= 33 \times 6 + 44\\
&= 33 \times 7 + 11 \qquad (33 \times 7 = 231).
\end{aligned}$$

En conclusion :

$$2222 = 330 \times 6 + 33 \times 7 + 11 = 33 \times 60 + 33 \times 7 + 11 = 33 \times 67 + 11.$$

On peut effectuer la division entière de 2222 par 33 d'une manière un peu plus efficace, voici comment. Commençons par noter que

$$33 \times 1 = 33,$$
$$33 \times 2 = 33 + 33 = 66,$$
$$33 \times 3 = 66 + 33 = 99,$$
$$33 \times 4 = 99 + 33 = 132,$$
$$33 \times 5 = 132 + 33 = 165,$$
$$33 \times 6 = 165 + 33 = 198,$$
$$33 \times 7 = 198 + 33 = 231,$$
$$33 \times 8 = 231 + 33 = 264,$$
$$33 \times 9 = 264 + 33 = 297.$$

Ensuite, on remarque que

$$33 \times 6 \times 10 = 1980 \leqslant 2222 < 2310 = 33 \times 7 \times 10,$$

et que

$$2222 = 1980 + 242 = 33 \times 6 \times 10 + 242 = 33 \times 60 + 242.$$

Puis, on remarque que

$$33 \times 7 = 231 \leqslant 242 < 264 = 33 \times 8,$$

et que

$$242 = 231 + 11 = 33 \times 7 + 11.$$

En conclusion :

$$2222 = 33 \times 60 + 33 \times 7 + 11 = 33 \times 67 + 11.$$

Ce dernier calcul peut être présenté schématiquement ainsi :

$$\begin{array}{r|l} 2222 & 33 \\ \cline{2-2} -1980 & 60 \\ \cline{1-1} 242 & \\ -231 & 7 \\ \cline{1-1} 11 & 67 \end{array} \quad \text{ou} \quad \begin{array}{r|l} 2222 & 33 \\ \cline{2-2} -1980 & 67 \\ \cline{1-1} 242 & \\ -231 & \\ \cline{1-1} 11 & \end{array} \quad \text{ou} \quad \begin{array}{r|l} 2222 & 33 \\ \cline{2-2} -198 & 67 \\ \cline{1-1} 242 & \\ -231 & \\ \cline{1-1} 11 & \end{array}$$

Exercice. Effectuer la division entière de trois cent douze par dix-huit en présentant tout le calcul, ainsi que les résultats, en base cinq.

I.14. PGCD et PPCM

Définition. Un nombre naturel d est dit un *plus grand commun diviseur* (*PGCD*) de nombres naturels a et b si et seulement si

(1) d est diviseur commun de a et b, et

(2) d est multiple de tout diviseur commun de a et b.

Autrement dit, un PGCD de a et b est un tel diviseur commun de a et b qu'il se factorise par tous les autres.

Observons que 1 est le PGCD de deux nombres naturels si et seulement si ces nombres sont premiers entre eux.

Exercice. Montrer que si a et b sont deux nombres naturels, et que c et d sont deux plus grands communs diviseurs de a et b, alors $c = d$.

Exemple. On peut montrer que 6 est le plus grand commun diviseur de 12 et 18. En effet, il n'y a que 4 diviseurs communs de 12 et 18 : 1, 2, 3 et 6, et 6 est multiple de chacun des autres.

Exercice. Trouver le PGCD de 0 et 0 (s'il existe).

Observons que pour tout nombre naturel a, le plus grand commun diviseur de a et 0 est a.

Définition. Un nombre naturel m est dit un *plus petit commun multiple* (*PPCM*) de nombres naturels a et b si et seulement si

(1) m est multiple commun de a et b, et

(2) m est diviseur de tout multiple commun de a et b.

Autrement dit, un PPCM de a et b est un tel multiple commun de a et b qu'il divise tous les autres.

Exercice. Montrer que si a et b sont deux nombres naturels, et que m et n sont deux plus petits communs multiples de a et b, alors $m = n$.

Exemple. On peut montrer que 30 est le plus petit commun multiple de 10 et 15.

Observons que pour tout nombre naturel a, le plus petit commun multiple de a et 1 est a.

Notation. Pour deux nombres naturels a et b, on va noter « $\mathrm{pgcd}(a, b)$ » l'unique plus grand commun diviseur de a et b (s'il existe), et « $\mathrm{ppcm}(a, b)$ » l'unique plus petit commun multiple de a et b (s'il existe).

Voici une propriété remarquable :

$$\mathrm{pgcd}(a,b) = a \quad \Leftrightarrow \quad a \mid b \quad \Leftrightarrow \quad \mathrm{ppcm}(a,b) = b.$$

En particulier, comme déjà observé,

$$\mathrm{pgcd}(a,0) = a = \mathrm{ppcm}(1,a),$$

car $1 \mid a \mid 0$.

Exercice. Soient a et b deux nombres naturels. Prouver que

$$\mathrm{pgcd}(a,\, \mathrm{ppcm}(a,b)) = a = \mathrm{ppcm}(a,\, \mathrm{pgcd}(a,b)).$$

Exercice. Soient a et b deux nombres naturels et d un diviseur commun de a et b. Prouver que

$$\mathrm{ppcm}(a,b) \times d \mid a \times b.$$

Indication : on peut écrire $a = d \times p$ et $b = d \times q$.

Remarque. Si a et b sont deux nombres naturels différents de 0, alors le plus petit commun multiple de a et b n'est pas leur *plus petit* commun multiple au sens usuel : comme 0 est multiple de tout nombre naturel, c'est 0 qui est le *plus petit* commun multiple de a et b au sens usuel. Pareil, le plus grand commun diviseur de deux nombres naturels n'est pas toujours le *plus grand* au sens usuel, car le plus grand commun diviseur de 0 et 0 est 0, mais tout nombre naturel est diviseur de 0, donc il n'y en a pas du *plus grand* au sens usuel.

Étudions les rapports entre le PGCD et l'ordre usuel ($\leqslant$) sur les diviseurs communs et entre le PPCM et l'ordre usuel sur les multiples communs.

Lemme. *Si un nombre naturel a divise un nombre naturel $b \neq 0$, alors $1 \leqslant a \leqslant b$.*

Démonstration. Soit q un nombre naturel tel que $a \times q = b$. Comme $b \neq 0$, on a que $a \neq 0$ et $q \neq 0$. Donc, $a \geqslant 1$ et $q \geqslant 1$, et $b \geqslant a \times 1 = a$. □

Corollaire. *Si a et b sont deux nombres naturels, c est un diviseur commun de a et b, d est le PGCD de a et b, et que $d \neq 0$, alors $d \geqslant c \geqslant 1$.*

Corollaire. *Si a et b sont deux nombres naturels, n est un multiple commun de a et b, m est le PPCM de a et b, et que $n \neq 0$, alors $1 \leqslant m \leqslant n$.*

On n'a pas encore répondu à la question suivante :

Question. Est-ce que tout couple de nombres naturels possède le PGCD et le PPCM ?

On verra que la réponse est affirmative. Le lemme suivant va nous aider traiter le cas du PGCD, et il sera aussi utilisé pour justifier un algorithme de calcul du PGCD.

Lemme. *Si a, b, c, q sont quatre nombres naturels tels que $a = b \times q + c$, alors*

(1) *tout diviseur commun de b et c est diviseur de a,*

(2) *tout diviseur commun de a et b est diviseur de c,*

(3) *en particulier,* $\mathrm{pgcd}(a,b) = \mathrm{pgcd}(b,c)$ *si* $\mathrm{pgcd}(a,b)$ *ou* $\mathrm{pgcd}(b,c)$ *existe.*

Exercice. Prouver ce lemme.

Ce lemme peut être utilisé pour calculer le PGCD de deux nombres naturels. Par exemple, utilisons le pour trouver le PGCD de 123 et 456 (et ainsi montrer qu'il existe). Pour cela, effectuons les divisions entières suivantes :

$$\begin{aligned}
456 &= 123 \times 3 + 87,\\
123 &= 87 \times 1 + 36,\\
87 &= 36 \times 2 + 15,\\
36 &= 15 \times 2 + 6,\\
15 &= 6 \times 2 + 3,\\
6 &= 3 \times 2 \quad (+0).
\end{aligned}$$

Comme 3 est le PGCD de 3 et 0 (ainsi que de 6 et 3), d'après le dernier lemme on obtient que

$$\begin{aligned}
\mathrm{pgcd}(456,\, 123) &= \mathrm{pgcd}(123,\, 87) = \mathrm{pgcd}(87,\, 36) = \mathrm{pgcd}(36,\, 15)\\
&= \mathrm{pgcd}(15,\, 6) = \mathrm{pgcd}(6,\, 3) = 3.
\end{aligned}$$

Cette méthode du calcul du PGCD s'appelle l'*algorithme d'Euclide*.

Exercice. Trouver le PGCD de 2222 et 333, s'il existe.

Il paraît clair que grâce au dernier lemme et à l'algorithme d'Euclide, on peut déterminer le PGCD de n'importe quels deux nombres naturels, et qu'en particulier, donc, n'importe quels deux nombres naturels admettent le PGCD. On peut prouver l'existence du PGCD rigoureusement et sans évoquer l'algorithme d'Euclide.

Théorème. *Quels que soient deux nombres naturels, leur PGCD existe.*

Démonstration. Démontrons ce théorème par un raisonnent *par l'absurde* : supposons qu'il existe deux nombres naturels qui n'ont pas du PGCD, et en déduisons une absurdité.

Supposons qu'il existe deux nombres naturels qui n'ont pas du PGCD. Dans ce cas, il existe deux nombres naturels qui n'ont pas du PGCD et dont la somme est la plus petite parmi les somme de tous les couples de nombres naturels qui n'ont pas du PGCD.

Soient donc a et b deux nombres naturels qui n'ont pas du PGCD et dont la somme est la plus petite parmi les sommes de tous les couples de nombres naturels qui n'ont pas du PGCD. Sans perte de généralité, supposons en plus que $a \geqslant b$. (Sinon on peut échanger les rôles de a et b).

Dans ce cas, $b \neq 0$, car $\text{pgcd}(a, 0) = a$. D'où, $(a - b) + b = a < a + b$, et donc il existe le PGCD de $a - b$ et b (d'après le choix de a et b). Or, d'après le dernier lemme, si le PGCD de $a - b$ et b existe, alors le PGCD de a et b existe aussi (et, en plus, $\text{pgcd}(a, b) = \text{pgcd}(a - b, b)$). Cela contredit le choix de a et b. □

On peut maintenant utiliser le théorème précédent d'existence du PGCD pour démontrer le théorème suivant d'existence du PPCM.

Théorème. *Quels que soient deux nombres naturels, leur PPCM existe.*

Pour démontrer ce théorème, les deux lemmes suivants seront utiles.

Lemme. *Si a, b, m, n sont quatre nombres naturels tels que m et n sont multiples communs de a et b, alors* $\text{pgcd}(m, n)$ *est également un multiple commun de a et b.*

Démonstration. Comme a et b sont diviseurs communs de m et n, ils divisent le PGCD de m et n. □

Lemme. *Si A est un ensemble non vide de nombres naturels, alors il existe un élément de A tel qu'aucun autre élément de A ne le divise.*

Démonstration. S'il n'y a qu'un seul nombre dans A, alors évidemment aucun autre élément de A ne le divise (car il n'y en a pas).

S'il y a au moins deux nombres dans A, alors au moins un nombre dans A est différent de 0. Soit a le plus petit nombre naturel non nul dans A. Alors aucun élément de A autre que a ne divise a.

Dans les deux cas, il y a un élément de A tel qu'aucun autre élément de A de le divise. □

Démonstration du théorème d'existence du PPCM. Soient a et b deux nombres naturels arbitraires. Évidemment, 0 est un de leurs multiples communs. (D'ailleurs, $a \times b$ l'est aussi.) Soit m un multiple commun de a et b tel qu'aucun autre multiple commun de a et b ne le divise. (Un tel m existe d'après le lemme précédent.) Montrons que $\text{ppcm}(a, b) = m$. Pour cela il ne reste qu'à prouver que m divise tout multiple commun de a et b.

Soit n un multiple commun arbitraire de a et b. D'après un lemme, $\text{pgcd}(m, n)$ est un multiple commun de a et b. (C'est grâce au théorème précédent qu'on sait que $\text{pgcd}(m, n)$ existe.) Cependant, $\text{pgcd}(m, n)$ divise m. Or, d'après le choix de m, aucun multiple commun de a et b different de m ne divise m. D'où, $\text{pgcd}(m, n) = m$, et donc m divise n. □

Grâce à ce théorème, pour montrer qu'un nombre naturel m est le PPCM de deux nombres naturels a et b, il suffit de vérifier que :

(1) m est un multiple commun de a et b, et que

(2) aucun autre multiple commun de a et b ne divise m.

Exemple. Clairement, 30 est un multiple commun de 10 et 15. Donc, le PPCM de 10 et 15 (qui existe, d'après le théorème) est diviseur de 30 et multiple de 10 et de 15. Les seuls multiples de 15 qui divisent 30 sont 15 et 30, et parmi ces deux, seulement 30 est multiple de 10. Donc, 30 est le PPCM de 10 et 15.

Il existe cependant une méthode plus directe pour calculer efficacement le PPCM de deux nombres naturels, la voici. On peut prouver[4] que si a et b sont deux nombres naturels premiers entre eux, alors $\text{ppcm}(a, b) = a \times b$. Il en résulte que pour tous nombres naturels a et b,

$$\text{ppcm}(a, b) \times \text{pgcd}(a, b) = a \times b.$$

I.15. Algorithme d'Euclide

Pour trouver le PGCD de deux nombres naturels, on peut utiliser l'*algorithme d'Euclide*, qui utilise la division entière (division euclidienne).

Soient a et b deux nombres naturels dont on cherche le PGCD. Posons

$$r_0 = a, \qquad r_1 = b.$$

Si $r_1 = b = 0$, alors $\text{pgcd}(a, b) = r_0 = a$. Sinon, posons q_2 et r_2 le quotient et le reste de la division entière de $r_0 = a$ par $r_1 = b$:

$$a = b \times q_2 + r_2, \qquad r_2 < b.$$

Ainsi,

$$r_0 = r_1 \times q_2 + r_2, \qquad r_2 < r_1.$$

Si $r_2 \neq 0$, on calcule le quotient q_3 et le reste r_3 de la division entière de $r_1 = b$ par r_2 :

$$r_1 = b = r_2 \times q_3 + r_3, \qquad r_3 < r_2.$$

On continue ainsi et détermine les quotients q_{k+2} et les restes r_{k+2} *par récurrence* :

$$r_k = r_{k+1} \times q_{k+2} + r_{k+2}, \qquad r_{k+2} < r_{k+1}.$$

On finira par trouver n tel que $r_{n+2} = 0$ et donc r_{n+1} divise r_n :

$$r_n = r_{n+1} \times q_{n+2}, \qquad r_{n+2} = 0.$$

Alors $\text{pgcd}(a, b) = r_{n+1}$. En effet, d'après un lemme précédent,

$$\begin{aligned}\text{pgcd}(a, b) = \text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2) = \cdots \\ = \text{pgcd}(r_n, r_{n+1}) = \text{pgcd}(r_{n+1}, 0) = r_{n+1}.\end{aligned}$$

[4] Une preuve habituelle passe par le *lemme de Bézout*.

I.16. PGCD et PPCM de familles arbitraires

En général, on définit le PGCD et le PPCM d'une n'importe quelle famille de nombres naturels de la même manière que dans le cas des couples :

- le PGCD d'une famille est le diviseur commun de cette famille qui est multiple de tout diviseur commun de cette famille,
- le PPCM d'une famille est le multiple commun de cette famille qui est diviseur de tout multiple commun de cette famille.

Par exemple :

$$\mathrm{pgcd}(36, 60, 90) = 6, \quad \mathrm{ppcm}(36, 60, 90) = 180.$$

Pour une famille (a) réduite à un seul nombre naturel a, on a :

$$\mathrm{pgcd}(a) = a = \mathrm{ppcm}(a).$$

Pour la *famille vide* () on a :

$$\mathrm{pgcd}() = 0, \quad \mathrm{ppcm}() = 1.$$

Les définitions du PGCD et du PPCM dans la section I.14 ont été données pour des couples de nombres naturels pour des raison pédagogiques, car à première vue une définition et un traitement plus généraux peuvent paraître plus complexes.

I.17. Nombres premiers et factorisation

Tout nombre naturel divise *zéro*, mais *zéro* ne divise que lui-même.

Le nombre *un* divise tous les nombres naturels, mais le seul nombre naturel qui le divise est *un* lui-même.

Ainsi, en ce qui concerne la relation de divisibilité pour les nombres naturels, les nombres *zéro* et *un* sont « les plus singuliers ».[5]

Cependant, certains autres nombres naturels, qui s'appellent les nombres *premiers*, se distinguent bien par rapport à la relation de divisibilité.

Définition. Un nombre naturel a est dit *premier*[6] si et seulement si

(1) a ne divise pas 1, et

(2) les seuls nombres naturels qui divisent a sont 1 et a.

[5] La relation de divisibilité ($|$) sur les nombres naturels est une *relation d'ordre*. Par rapport à cette relation d'ordre, 0 est le plus grand nombre, et 1 est le plus petit.

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

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

On peut séparer les nombres naturels strictement plus grands que 1 en premiers et en composés par le *crible d'Ératosthène*.

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

Exercice. Prouver cette proposition.

On peut prouver que si un nombre naturel est décomposé en un produit de nombres premiers de deux façons différentes, les deux décompositions ne diffèrent que par l'ordre des facteurs. Par exemple,

$$60 = 2 \times 2 \times 3 \times 5 \quad \text{et} \quad 60 = 3 \times 2 \times 5 \times 2.$$

Ce fait s'appelle le *théorème fondamental de l'arithmétique*, on l'énonce ici sans démonstration.[7]

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

Voici un exemple d'un problème non résolu (jusqu'en 2024) en arithmétique :

Conjecture (*Conjecture de Goldbach*)**.** *Tout nombre naturel pair strictement supérieur à 2 s'écrit comme la somme de deux nombres premiers.*

Question. La conjecture de Goldbach, est-elle vraie ou fausse ?

[6] 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 naturels, 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.

[7] Une preuve habituelle passe par le *lemme de Bézout*.