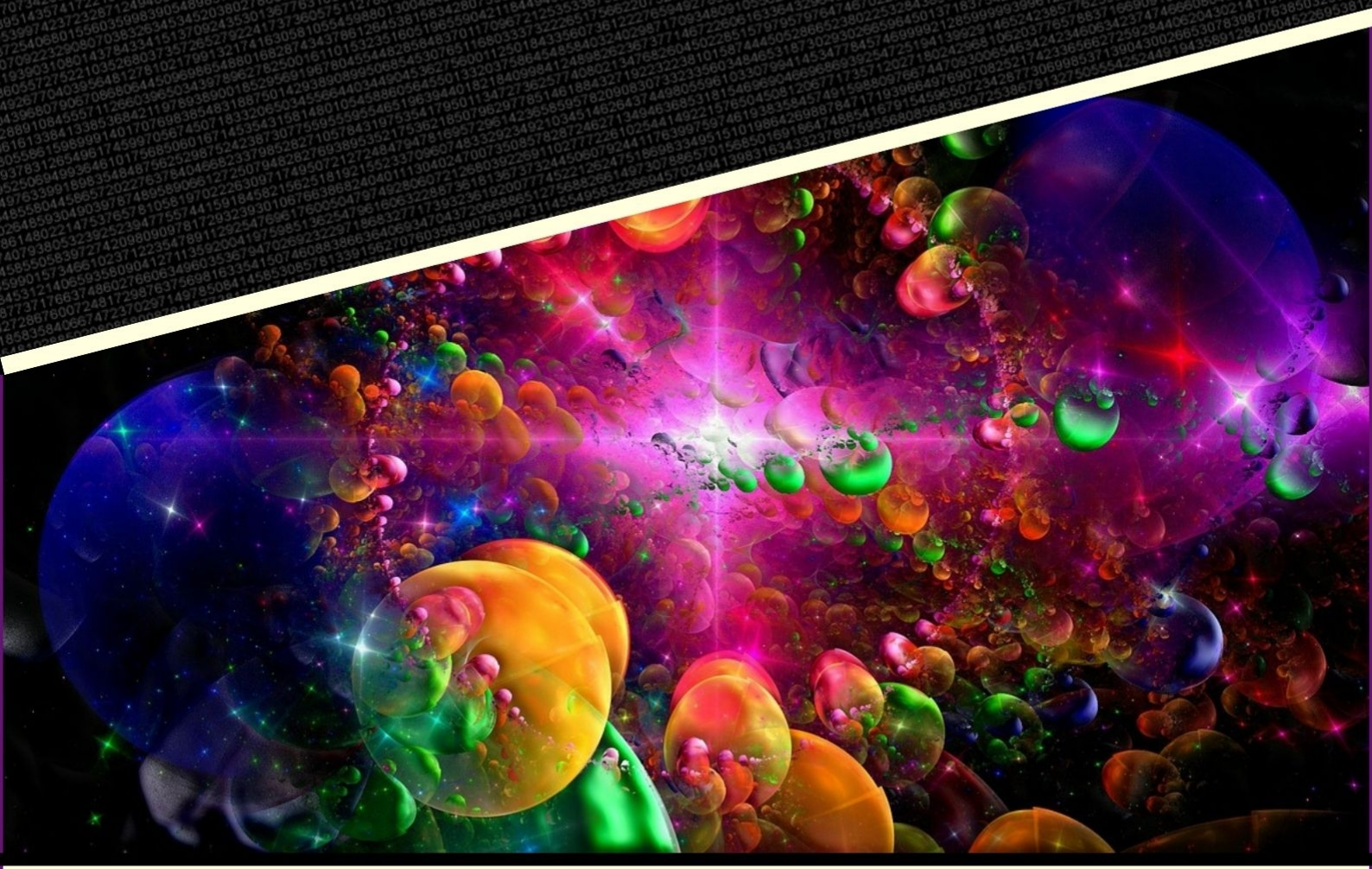
# ARITHMÉTIQUE ÉLÉMENTAIRE



## Des nombres entiers naturels aux nombres rationnels

MATHESIS
l'Univers Mathématique
1ère année, Semestre I, Cours n°3

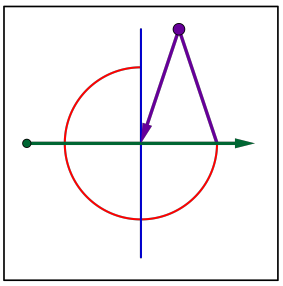
Jean Barbet

# Arithmétique Elémentaire

## Des Nombres Entiers Naturels aux Nombres Rationnels

Jean Barbet

**M A T H E S I S**
*l'Univers Mathématique*
1ère année — Semestre I — Cours no 3



La Règle et le Compas : www.reglecompas.fr

# Avant-propos

## Présentation de l'auteur

Je m'appelle Jean Barbet, je suis mathématicien indépendant et enseignant en ligne. Docteur en mathématiques, je me suis réorienté après des études en sciences de la vie. A cause de lacunes universitaires j'ai rencontré mes premières difficultés et mes premiers échecs en mathématiques. Pour réussir ma reconversion, j'ai du retravailler par moi-même dans les manuels de référence, choisir ce qui était essentiel, intégrer les connaissances et la pratique, et trouver un sens aux différentes disciplines mathématiques et un lien entre elles, parce que je n'avais pas le temps de refaire tout ce qui m'avait manqué.
J'ai suivi la même méthode pour achever mes études et c'est celle que j'utilise aujourd'hui pour apprendre et créer des mathématiques. La science mathématique possède un sens en elle-même et forme une unité, et ses différents domaines sont profondément liés. Prendre ceci en compte permet d'apprendre, d'assimiler et de comprendre de manière naturelle le noyau de la connaissance mathématique supérieure et tout ce travail m'a permis de compléter mon cursus universitaire jusqu'au Doctorat en mathématiques (obtenu en 2010).
Après plus de dix années d'expérience dans l'enseignement des mathématiques, du collège à l'université et à l'école d'ingénieurs, j'ai rassemblé les résultats de ma synthèse dans un corpus du niveau de la Licence universitaire : Mathesis, l'Univers Mathématique. Avec Mathesis, je veux donner la possibilité, à quiconque veut apprendre sérieusement des mathématiques, d'acquérir le noyau de ce qu'on appelle la mathématique supérieure, c'est-à-dire celle qu'on fait après le lycée et qui correspond à la science mathématique moderne, avec ses concepts et ses méthodes.

## Mathesis - l'Univers Mathématique

Le corpus intègre l'essentiel de ce qu'on trouve dans une Licence de mathématiques à l'université, ainsi que des compléments substantiels. Il se divise en trois années, de deux semestres chacune. Il sera publié sous la forme de fascicules correspondant chacun à un cours. Chaque semestre aborde en cinq ou six cours l'ensemble des disciplines et les fascicules. J'ai voulu éviter les écueils habituels liés aux contraintes de l'organisation de l'enseignement supérieur : des cours séparés dans des domaines étanches (Algèbre, Analyse...) et exposant des notions abstraites déconnectées de l'intuition, des exercices techniques trop difficiles et dépourvus de sens.
Dans Mathesis, l'abstraction mathématique, inévitable, est construite pas-à-pas

à partir de l'intuition concrète, comme on apprend aux jeunes enfants au cours élémentaire. Il n'y a pas de domaine étanche, ni plusieurs séries de manuels pour chaque domaine, mais un cursus unique, qui revient cycliquement sur chaque sujet en insistant sur les liens qu'ils entretiennent. Rien n'empêche cependant de choisir un sujet et de ne lire que les fascicules qui s'y rapportent. La pratique, essentielle, est intégrée à la théorie, en ce que des exercices d'un niveau abordable mettent en œuvre directement, à chaque section, ce qui a été exposé dans le cours, et complètent l'apprentissage par l'application des connaissances générales à des situations particulières naturelles.
La **méthode de travail** que je vous conseille est la même pour tous les cours : chaque section correspond à une leçon, et l'étudiant(e) devrait la lire une fois tranquillement, en essayant de la comprendre ; la prise de notes personnelles est recommandée, mais pas indispensable : vous pouvez aussi annoter votre cours. Lorsqu'il y a des démonstrations, il/elle est invité(e) à les analyser et à les refaire, et lorsqu'il y a des exercices, à les chercher systématiquement. Avant de commencer chaque nouvelle section, il vous faudra relire la précédente pour vous remémorer le travail accompli et vous mettre en condition.
Mathesis vous propose un apprentissage sans échec : pour construire votre connaissance mathématique il n'est pas nécessaire d'apprendre par cœur le cours ni les démonstrations (il suffit de les analyser), et il n'est pas nécessaire de trouver la solution des exercices et des problèmes (il suffit de les chercher honnêtement). L'effort sérieux et régulier est cumulatif et suffit à l'assimilation : apprendre des mathématiques est à la portée de tous, même il s'agit d'une tâche exigeante, qui demande de la persévérance. Chaque section ou leçon demande entre trente minutes et une heure de travail par jour ; à cinq jours par semaine, chaque cours demande environ un mois. Si les leçons sont trop longues, n'hésitez pas à les fractionner : il vaut mieux travailler un peu tous les jours selon sa capacité, plutôt que s'épuiser et espacer les séances d'étude.

# Présentation du cours

Cet ouvrage est le troisième volume de la série, il s'agit donc du $3^{\text{ème}}$ cours du semestre I de la $1^{\text{ère}}$ année. Structuré en trois chapitres, il est divisé en 19 sections ou leçons et comporte 18 figures. Il traite de toute l'arithmétique (ou théorie des nombres) élémentaire, à partir d'une description axiomatique des trois ensembles $\mathbb{N}$ (des nombres entiers naturels), $\mathbb{Z}$ (des nombres entiers relatifs) et $\mathbb{Q}$ (des nombres rationnels), et des relations organiques et structurelles entre eux.
Dans le second volume, "Ensembles, Applications et Numération", nous avons complété les bases de théorie naïve des ensembles, conceptualisé la notion de "fonction mathématique" via celle d'application, et grâce à la notion de *bijection* nous avons pu d'une part définir et dénombrer les ensembles finis, d'autre part définir et caractériser les ensembles infinis.
Dans ce troisième volume, nous entrons de plain pied dans le coeur de la science mathématique moderne, en posant les fondements de l'arithmétique ou théorie des nombres, dans le cadre conceptuel de la théorie naïve des ensembles élaboré dans les cours précédents. Le cours commence ainsi par la description *axiomatique*

de l'ensemble $\mathbb{N}$ des entiers naturels par les propriétés de la fonction successeur, évoquées au cours n$^o$ 2 à propos des ensembles infinis, et rassemblées dans les *axiomes de Peano*.
A partir de cette description simple on redéfinit toute la "structure arithmétique" (addition, multiplication, ordre naturel et divisibilité) de l'ensemble $\mathbb{N}$, et on aborde solidement les questions de divisibilité, sujet de l'arithmétique, à travers la division euclidienne, les nombres premiers (dont on démontre l'infinité dans le célèbre théorème d'Euclide) et les nombres premiers entre eux; on propose également une étude sommaire des bases de numération.
L'absence d'opposés additifs dans l'ensemble $\mathbb{N}$ limite les possibilités de la théorie des entiers : c'est l'occasion d'introduire, aussi grâce à une description axiomatique simple fondée sur l'addition, l'ensemble $\mathbb{Z}$ des nombres entiers relatifs, où l'existence d'une soustraction simplifie radicalement la théorie arithmétique et lui donne toute son ampleur. Cette théorie culmine ici avec le théorème de Bézout sur les nombres premiers entre eux, qui permet d'aborder solidement le théorème "fondamental de l'arithmétique" de Gauss, lequel a trait à la décomposition des entiers naturels en nombres premiers. Ici, la *valeur absolue* joue un rôle intéressant dans le rapport entre les ensembles $\mathbb{N}$ et $\mathbb{Z}$.
En introduisant l'ensemble $\mathbb{Q}$ des nombres rationnels, à nouveau par une description axiomatique très simple et fondée sur la multiplication, nous franchissons une frontière à la fois arithmétique et géométrique. L'existence d'un inverse multiplicatif pour tout rationnel non nul change l'approche de l'arithmétique : l'étude de la divisibilité disparaît au profit de celle de la structure multiplicative des rationnels, qui transparaît dans la *décomposition des nombres rationnels* positifs en facteurs premiers, possible grâce aux puissances négatives des rationnels. Les propriétés arithmétiques de l'ensemble $\mathbb{Q}$ se traduisent alors également de manière géométrique : la partie entière et la propriété d'Archimède se déduisent de la division euclidienne, et l'étude de la *commensurabilité* des grandeurs rationnelles, qui prépare la théorie des nombres réels du cours suivant, est rapportée aux nombres premiers entre eux.
Avec ce troisième cours s'achève la première moitié du premier semestre, et nous avons posé les fondements logiques et arithmétiques essentiels au semestre et au cursus. La transition vers la seconde partie du semestre, dédiée à la géométrie euclidienne, à l'analyse (théorie des suites et des fonctions de nombres réels) et à l'algèbre (nombres complexes, espaces de dimension supérieure, quaternions...), est assurée par le "continuum arithmético-géométrique" émergeant de la théorie des nombres rationnels.

Jean Barbet, 6 décembre 2021

# Compléments sur la méthode de travail

**Comprendre le cours** L'intégration du cours ne nécessite pas d'apprendre par cœur. Par contre, une simple lecture est insuffisante. Lorsqu'un enseignant donne un cours en direct, il insiste sur certains points, donne des explications supplémentaires. Ces éléments ne sont pas disponibles dans le cours écrit, il est donc nécessaire que l'étudiant(e) y supplée, ce qui est à sa portée ; il (elle) doit faire ce qu'on appelle une lecture analytique. Dans un cours de mathématiques, on distingue plusieurs parties : outre les exercices et problèmes, nous avons des explications, des définitions, des propositions et des exemples.

Les explications sont le corps du texte mathématique : on introduit un nouveau sujet, on expose les propriétés d'un nouvel objet. Il faut lire ce texte en se posant la question : est-ce que je comprends ce que je lis ? Si ce n'est pas le cas, il faut s'arrêter et chercher les réponses : soit nous n'avons pas compris le texte lui-même, soit nous sommes mal assurés relativement à un point exposé dans une section précédente ; il nous faut alors y revenir pour clarifier notre pensée.

Les définitions introduisent de nouveaux objets ou de nouvelles notions, toujours à partir d'objets ou de notions introduits précédemment. Comme pour le corps du texte, il faut s'assurer de bien comprendre les définitions, les analyser en détail et revenir à des sections précédentes si nécessaire. Parfois, certains notions du lycée ou du collège sont utilisées de manière intuitive, sans être redéfinies immédiatement : l'étudiant(e) les retrouvera facilement par ses propres moyens.

Les propositions (appelées propositions, théorèmes, lemmes et corollaires) énoncent des propriétés essentielles des objets dont traite le cours, ceux qui précisément constituent la connaissance mathématique propre, celle qu'on met en évidence. Comme pour les définitions, il faut s'assurer de bien en comprendre les énoncés, mais à la différence des définitions il faut aussi en comprendre les démonstrations. Une démonstration est une argumentation mathématique, qui cherche à établir la véracité de la proposition énoncée. Il faut l'analyser, c'est-à-dire en identifier les différentes parties et leurs articulations logiques, et chercher à en comprendre chaque partie, et comment toutes les parties s'agencent pour établir le résultat annoncé. Une fois une démonstration comprise, il est bon de chercher à la reproduire soi-même.

Les exemples servent à illustrer les nouveaux concepts introduits par les définitions, ou bien les propriétés démontrées dans les propositions. Ces concepts et propriétés sont en effet la plupart du temps des généralités : il est donc important de comprendre comment ils se réalisent ou se manifestent dans des cas particuliers. Les exemples sont à bien comprendre également.

L'étudiant(e) qui veut faire des fiches devrait prendre en note surtout les définitions et les énoncés des propositions. Quelques exemples choisis parmi les plus suggestifs peuvent illustrer utilement ses notes. Enfin, il est bon, avant de commencer une nouvelle séance d'étude, de relire le cours étudié à la session précédente ou de relire ses notes, pour se remémorer les concepts et propriétés étudiés juste avant. Comme tout apprentissage, l'apprentissage mathématique est cumulatif.

**Travailler les exercices** Les exercices mathématiques consistent à mettre en œuvre ou appliquer le cours dans des situations particulières. Les problèmes sont des exercices d'un niveau supérieur qui consistent à résoudre une question ou une série de questions en faisant preuve de plus de créativité. Il n'est pas toujours possible de trouver la solution d'un exercice ou d'un problème à la première tentative ; on peut même échouer régulièrement. Aussi surprenant soit-il, l'important dans la recherche de la solution d'un exercice ou d'un problème n'est pas de trouver la solution, mais de la chercher honnêtement.
La résolution d'un exercice ou d'un problème consiste à développer une stratégie et à la mettre en œuvre. La première étape consiste à analyser l'exercice ou le problème : il faut s'assurer qu'on en comprend tous les termes, et qu'on comprend la question posée ; cette étape est essentielle et est une première mise en œuvre du cours. La seconde étape consiste à élaborer une stratégie : en fonction de la question posée, il faut identifier les idées qui nous viennent à l'esprit, souvent de manière désordonnée, et inventer une série d'étapes pour aboutir à la réponse ; souvent, il faut identifier comment les éléments du cours présents dans l'énoncé peuvent être utilisés pour atteindre l'objectif. La troisième étape consiste à mettre en œuvre la stratégie : il faut faire un ou des calcul(s), un ou des raisonnement(s), de manière rigoureuse. La seconde et la troisième étapes se font souvent simultanément ; il n'est en général possible d'analyser la démarche adoptée qu'après avoir effectué une tentative.
On a cherché l'exercice ou le problème honnêtement quand on est allé aussi loin qu'on le peut. Parfois, l'analyse de la question s'avère déjà difficile, et on n'a pas d'idée pour la résoudre. Parfois une stratégie nous vient à l'esprit, mais il nous manque l'adresse nécessaire pour aboutir, soit raisonner ou calculer efficacement ; ou alors, la stratégie est incomplète ou erronée. Parfois enfin, on arrive jusqu'au bout ; si c'est la situation la plus satisfaisante, ce n'est toutefois pas toujours le cas : la difficulté est inhérente à la mathématique, et à l'impossible nul n'est tenu. Lorsqu'on n'aboutit pas à la solution du problème, on peut (et on devrait) y revenir ultérieurement. Mais il est possible de chercher honnêtement la solution de chaque exercice, le minimum étant l'analyse de la question posée ; celle-ci est en principe toujours accessible, si bien qu'on n'échoue à l'exercice que lorsqu'on renonce à se poser la question.

# Table des matières

# Chapitre 1

# L'ensemble $\mathbb{N}$ des nombres entiers naturels

Dans ce premier chapitre, nous abordons l'étude *axiomatique* de l'ensemble $\mathbb{N}$ des nombres entiers naturels. Dans le cours n$^o$ 1, nous avons considéré que les nombres entiers naturels et leurs propriétés élémentaires nous étaient connus de manière *intuitive*, et qu'ils étaient ainsi des concepts mathématiques *primitifs*, au sens où on ne les définit pas mathématiquement.
Nous conservons ici ce point de vue, et l'approche qui consiste à théoriser les propriétés des entiers naturels grâce à la théorie des ensembles, en considérant des propriétés globales de l'ensemble $\mathbb{N}$. Il est toutefois possible de réduire les propriétés qu'on doit admettre comme des principes indémontrables à un petit jeu de trois *axiomes* qu'on doit au mathématicien Giuseppe Peano.
Nous allons voir comment, à partir de ces principes simples et transparents concernant la fonction successeur, il est possible de définir toute la "structure naturelle" de l'ensemble $\mathbb{N}$, et de développer des bases solides de l'arithmétique ou théorie des nombres. D'ailleurs, même si nous ne définissons pas mathématiquement les nombres entiers naturels, les axiomes de Peano déterminent cet ensemble de manière "essentiellement unique", et c'est tout ce qu'il nous faut en mathématique.

## 1.1 Les axiomes de Peano comme postulats

Lorsque nous avons défini la notion d'ensemble infini dans le cours sur le fini et l'infini (cours n$^o$ 2 du semestre I), l'ensemble $\mathbb{N}$ des nombres entiers naturels a joué un rôle essentiel, à la fois comme "frontière" entre les ensembles finis et infinis, et comme exemple fondamental d'ensemble infini permettant de caractériser, c'est-à-dire d'identifier, tous les autres. Pour montrer que $\mathbb{N}$ est infini, nous avons du faire usage du *principe de récurrence*, qui est en quelque sorte une propriété de la fonction successeur $s : \mathbb{N} \to \mathbb{N}$. Nous allons ici l'exposer précisément et l'exploiter pour décrire l'ensemble $\mathbb{N}$ et fonder notre étude de l'arithmétique élémentaire.
Il est possible de rassembler des propriétés essentielles de la fonction successeur, appelées "axiomes", qui permettent de la décrire complètement, et à partir de là, de "reconstituer" toute la "structure" opératoire ($+$ et $\times$) et relationnelle ($\leq$ et $|$) classique de l'ensemble $\mathbb{N}$.

### 1.1.1 Les axiomes de l'arithmétique de Peano

La liste d'axiomes que nous présentons dans cette section est due au mathématicien italien Giuseppe Peano. L'idée sous-jacente à cette démarche "axiomatique" est que l'usage que nous avons fait de la fonction successeur repose sur des propriétés intuitives, indémontrables : ces propriétés déterminent en fait ce que nous "entendons" par la fonction successeur !
Au point de vue où nous nous plaçons, nous devrions peut-être plutôt appeler ces propriétés des *postulats* : elles dénotent ce que nous affirmons, ce que nous "croyons", à propos de la fonction successeur. Quoiqu'il en soit, ces axiomes ou postulats sont des conditions sous lesquelles nous pouvons fonder la mathématique comme science, en commençant par l'arithmétique. Ces conditions sont nécessaires, au sens où nous n'avons pas le choix d'adopter une telle démarche pour bâtir les mathématiques : si nous rejetons ces axiomes, ou ce point de départ, il nous faudra en trouver d'autres, équivalents.
Nous choisissons ici des axiomes simples, naturels et éprouvés, à propos de la fonction la plus simple possible sur le premier ensemble naturel de nombres.

**Axiome 1.1.1.** $0$ *n'est le successeur d'aucun entier naturel. En d'autres termes, il n'existe pas d'entier naturel* $n$ *tel que* $s(n) = 0$.

Cet axiome dit en particulier que la fonction $s$ *n'est pas surjective*, puisque le nombre $0$ ne possède pas d'antécédent par $s$.

**Axiome 1.1.2.** *Si deux entiers naturels* $m$ *et* $n$ *ont le même successeur, alors ils sont égaux. En d'autres termes, pour tous entiers naturels* $m, n$, *si* $s(m) = s(n)$ *alors* $m = n$.

On peut reformuler cet axiome en disant que l'application successeur *est injective*. Sa co-restriction à son image est donc une bijection de $\mathbb{N}$ sur une partie propre de $\mathbb{N}$ : on reconnait ici la caractérisation intrinsèque d'un ensemble infini, que nous avons abordée à la fin du cours sur le fini et l'infini.
Quelle est l'image $Im(s)$ de l'application successeur ? Pour le déterminer, il nous faut là encore faire appel à notre intuition. Or, il paraît évident que tout entier naturel non nul est le successeur d'un entier naturel ! Nous pourrions l'introduire comme un nouvel axiome, mais il s'agit d'une conséquence de l'axiome suivant, dit "principe de récurrence" :

**Axiome 1.1.3** (Principe de récurrence (ou d'induction))**.** *Si* $S$ *est un sous-ensemble de* $\mathbb{N}$ *tel que :*
*i)* $0 \in S$
*ii) pour tout* $n \in S$, $s(n) \in S$ *("étape de récurrence"),*
*alors on a* $S = \mathbb{N}$.

Les applications de ce principe, ubiquitaires dans toute la mathématique, clarifieront sa signification et sa fécondité, mais il exprime intuitivement que l'ensemble $\mathbb{N}$ est entièrement "parcouru" si nous l'énumérons à partir de 0 et ajoutons chaque entier naturel successif, de manière indéfinie. On peut en déduire la détermination de l'image de $s$ :

**Proposition 1.1.4.** *Si on admet le principe de récurrence, alors l'image de $s$ est $\mathbb{N}^*$, l'ensemble des entiers naturels non nuls.*

*Démonstration.* Soit $S$ l'ensemble $\{0\} \cup Im(s) = \{0\} \cup \{n \in \mathbb{N} : \exists m \in \mathbb{N},\ n = s(m)\}$. Si nous montrons que $S = \mathbb{N}$, alors tout entier naturel non nul est dans l'image de $s$, donc $Im(s) = \mathbb{N}^*$. Par définition, on a $0 \in S$, et supposons que $n$ est un entier naturel, et que $n \in S$. Par définition, l'entier naturel $s(n)$ est dans $S$ ! Par le principe de récurrence, l'ensemble $S$ est $\mathbb{N}$ tout entier, et la proposition est démontrée. □

Rappelons que le successeur $s(n)$ d'un entier naturel $n$ est l'entier naturel que nous notons aussi $n+1$, étant entendu que 1 est le successeur de 0. En effet, lorsque nous définirons dans la suite l'addition à partir du successeur, nous verrons que $s(n)$ est *par définition* égal à $n + 1$.
Le principe de récurrence est essentiellement utilisé en mathématique de deux manières différentes, que nous avons déjà rencontrées et pratiquées : pour les démonstrations par récurrence d'une part, pour les définitions par récurrence d'autre part.
Une **démonstration par récurrence** consiste à démontrer qu'une propriété $P(n)$, qui dépend de l'entier naturel $n$, est vraie quel que soit $n \in \mathbb{N}$, c'est-à-dire universellement valide. Cela revient à démontrer que l'ensemble $S$ des entiers naturels $n$ qui ont la propriété $P(n)$, soit $S = \{n \in \mathbb{N} : P(n)\}$, est $\mathbb{N}$ tout entier. Le raisonnement par récurrence consiste alors à appliquer le principe de récurrence à l'ensemble $S$.

### 1.1.2 Le théorème de récurrence

En ce qui concerne les **définitions par récurrence**, l'explication est un peu plus délicate et la justification repose sur le *théorème de récurrence* que nous exposons ci-après. La définition par récurrence consiste essentiellement à "construire" une application $u$ de $\mathbb{N}$ dans un ensemble $E$ (ce qu'on appelle une *suite* d'éléments de $E$) à partir de deux données :
i) Le choix du "premier terme" de la suite, c'est-à-dire $u(0)$, qui est un élément donné de $E$
ii) Un "procédé" de définition de la valeur $u(n+1)$ de la suite au rang $s(n) = n+1$ lorsqu'on connaît sa valeur $u(n)$ au rang $n$.
La seconde donnée peut se formaliser comme celle d'une application $f$ de $E$ dans lui-même : une telle fonction fournit bien un moyen de "transformer" une valeur $u(n)$ de la suite en un autre élément de $E$, même si dans cette approche la fonction $f$ comme procédé est définie pour tous les éléments de $E$, tandis qu'on n'en a besoin *a priori* que pour les valeurs de la suite. Ceci explique la formulation du théorème suivant, dont la démonstration est un peu exigeante mais très instructive :

**Théorème 1.1.5** (Théorème de récurrence)**.** *Si $f : E \to E$ est une application d'un ensemble dans lui-même et $a \in E$, il existe une unique application $g : \mathbb{N} \to E$ telle que $g(0) = a$ et $g(s(n)) = f(g(n))$ pour tout $n \in \mathbb{N}$.*

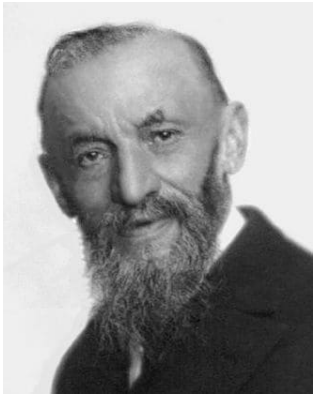
*Démonstration.* La démonstration se fait en deux étapes.
i) On montre par récurrence que pour tout $n \in \mathbb{N}$, il existe une unique application $h : [[0, n]] \to E$ telle que $h(0) = a$ et pour tout $i < n$, $h(s(i)) = f(h(i))$. Pour $n = 0$,

la seule fonction $h : [[0,0]] = \{0\} \to E$ telle que $h(0) = a$ (la deuxième condition est "vide") est définie par cette condition, donc la propriété est vérifiée au rang $n = 0$. Supposons qu'elle le soit au rang $n$ : il existe une unique fonction $h : [[0,n]] \to E$ telle que $h(0) = a$ et $h(s(i)) = f(h(i))$ pour tout $i < n$. Définissons une fonction $g : [[0,n+1]] \to E$ en posant $g(i) = h(i)$ pour tout $i < n+1$ et $g(n+1) = f(h(n))$. On a $g(0) = h(0) = a$, et pour tout $i < n$, $g(s(i)) = h(s(i)) = f(h(i))$ par l'hypothèse de récurrence; comme $g(s(n)) = f(g(n))$ par définition, $g : [[0,n+1]] \to E$ possède la propriété voulue. Supposons que $k : [[0,n+1]] \to E$ soit une autre fonction avec ces propriétés : en particulier, on a $k(0) = a$ et pour tout $i < n$, $k(s(i)) = f(k(i))$ et par hypothèse de récurrence, $h$ étant unique avec ces propriétés la restriction $k|_{[[0,n]]}$ de $k$ à $[[0,n]]$ est égale à $h$. Il s'ensuit aussi que $k(n+1) = k(s(n)) = f(k(n)) = f(h(n)) = f(g(n)) = g(s(n)) = g(n+1)$, donc finalement $k = g$ et l'unicité aussi est démontrée au rang $n+1$. On conclut par récurrence que la propriété est vérifiée pour tout $n \in \mathbb{N}$.
ii) On en déduit qu'il existe une unique application $g : \mathbb{N} \to E$ telle que $g(0) = a$ et pour tout $n \in \mathbb{N}$, $g(s(n)) = f(g(n))$. Pour cela, soit $n \in \mathbb{N}$ : par (i) il existe une unique fonction $h_n : [[0,n]] \to E$ avec les propriétés données, et on définit alors $g(n)$ comme $h_n(n)$. On obtient ainsi une fonction $g : \mathbb{N} \to E$. Par définition, on a $g(0) = h_0(0) = a$, et pour tout $n \in \mathbb{N}$, on a $g(s(n)) = h_{s(n)}(s(n)) = f(h_{s(n)}(n)) = f(h_n(n))$ (car par unicité dans (i), on a $h_{s(n)}|_{[[0,n]]} = h_n$) $= f(g(n))$, donc $g$ a les propriétés voulues. En ce qui concerne l'unicité, si $k : \mathbb{N} \to E$ est une application telle que $k(0) = a$ et $k(s(n)) = f(k(n))$ pour tout $n \in \mathbb{N}$, on démontre facilement par récurrence que $\{n \in \mathbb{N} : g(n) = k(n)\}$ est l'ensemble $\mathbb{N}$ tout entier, et donc que $k = g$, et le théorème est démontré. □

Dans la pratique, la définition par récurrence procède par une "construction" du graphe $R$ de la suite $g$, soit une relation fonctionnelle $R$ sur $\mathbb{N} \times E$, pour laquelle pour tout $n \in \mathbb{N}$, il existe $x \in E$ avec $(n,x) \in R$. En principe, on définit $g(0)$ (on choisit un élément $a$ de $E$), à partir d'une propriété essentielle, et on décrit un procédé (la fonction $f$) qui permet de définir $g(n+1)$ à partir de $g(n)$, sous la forme d'une expression qui traduit les contraintes de définition de la fonction $g$. Par le théorème 1.1.5, l'unique fonction $g$ ayant les propriétés désirées est la suite qu'on définit par récurrence.

**Exemple 1.1.6.** Reprenons la définition par récurrence de l'expression $a^n$, pour $a$ un nombre réel et $n$ un entier naturel : on pose $a^0 := 1$ et $a^{n+1} = a^n \times a$. Dans cette situation, on définit une application $g : \mathbb{N} \to \mathbb{R}$, qui associe à l'entier $n$ le nombre réel $a^n$. L'application $f : \mathbb{R} \to \mathbb{R}$ qui convient est la "multiplication par $a$", qui associe à $x \in \mathbb{R}$ le nombre réel $a.x$. En posant $g(0) = 1$ (valeur de $a^0$), le théorème 1.1.5 nous assure qu'il existe une seule fonction $g : \mathbb{N} \to \mathbb{R}$ telle que $g(0) = a$ et $g(n+1) = a.g(n)$ pour tout $n \in \mathbb{N}$ : c'est la fonction cherchée.

Terminons en précisant que la description de la fonction successeur par ces axiomes suppose qu'il est légitime, dans la théorie des ensembles ou le méta-univers, de poser l'existence d'une application de $\mathbb{N}$ dans lui-même ayant ces propriétés. Admettre l'existence d'un ensemble $\mathbb{N}$ de tous les entiers naturels est d'ailleurs déjà une supposition de ce genre, que nous complétons ici : nous (sup)posons - sans pouvoir le démontrer - qu'il est licite de travailler avec une telle fonction dans l'univers des



Giuseppe Peano, mathématicien et linguiste italien.

objets mathématiques.
A la racine de l'édifice mathématique, comme de tout discours scientifique, il faut faire un "pas de foi" dans la cohérence des principes élémentaires sur lesquels il faut bâtir, et qu'il n'est jamais possible de démontrer; ceci souligne que la créativité demeure un élément essentiel de l'activité scientifique, mathématique en particulier. Grâce à ces quelques axiomes très simples, nous entrons avec la théorie naïve des ensembles et l'axiomatique de Peano dans la construction rigoureuse de tout l'édifice mathématique : nous allons voir qu'il est désormais possible de définir toute la structure arithmétique naturelle et d'en redémontrer les propriétés élémentaires. La suite du semestre montrera également comment on peut "décrire" par la méthode axiomatique tous les autres ensembles naturels $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ et $\mathbb{H}$ abordés au premier et au second cours, à partir de la structure de $\mathbb{N}$ et de la théorie naïve des ensembles.

## Exercices de la section

*Exercice* 1.1.7. Justifier le principe du raisonnement par récurrence à l'aide l'axiome 1.1.3. Autrement dit, si $P(n)$ est une propriété des entiers naturels $n$, telle que $P(0)$ est vraie, et telle que l'implication $P(n) \Rightarrow P(n+1)$ est universellement valide, expliquer pourquoi $P(n)$ est universellement valide, c'est-à-dire pourquoi l'énoncé $\forall n \in \mathbb{N}, P(n)$ est vrai.

*Problème* 1.1.8. On se propose ici de démontrer la "catégoricité" de l'axiomatique de Peano, autrement que la fonction successeur décrit de manière essentiellement "unique" l'ensemble $\mathbb{N}$. Plus précisément, il s'agit de montrer que si $E$ est un ensemble quelconque et $f : E \to E$ est une application qui possède les mêmes propriétés que le successeur, à savoir :
a) il existe $x \in E$ tel que $x \notin Im(f)$
b) $f$ est injective
c) si $S$ est une partie de $E$ telle que $x \in E$ et $f(y) \in S$ dès que $y \in S$, on a $S = E$,
alors $(E, f)$ est "isomorphe à $\mathbb{N}$", c'est-à-dire qu'il existe une bijection $g : \mathbb{N} \to E$ telle que $g^{-1} \circ f \circ g = s$. Cela signifie que sur le plan mathématique, $s$ et $f$ sont "indiscernables".
i) On définit $g : \mathbb{N} \to E$ en posant $g(0) = x$ et pour tout $n \in \mathbb{N}$, $g(n+1) = f(g(n))$. Montrer que $g$ est définie sur tout l'ensemble $\mathbb{N}$.

ii) Soit $S = Im(g)$. En utilisant la propriété (c) de $f$, montrer que $g$ est surjective.
iii) Soit l'ensemble $S = \{n \in \mathbb{N} : \forall m < n,\ g(m) \neq g(n)\}$. Démontrer que $S = \mathbb{N}$, et en conclure que $g$ est injective. Indication : pour l'hypothèse de récurrence, distinguer les cas $m = 0$ et $m > 0$.
iv) Conclure en exprimant $g^{-1} \circ f \circ g$.

## 1.2 Structure opératoire de l'ensemble $\mathbb{N}$

### 1.2.1 Définition de l'addition

Jusqu'à maintenant, nous avons usé de descriptions intuitives des propriétés de $+$, $\times$, $<$ et $\leq$ sur les entiers naturels; seule la relation de divisibilité $|$ a été définie à partir de la multiplication dès le premier cours du semestre I.
Il est possible de "réduire" toutes ces opérations et relations à la seule fonction successeur, c'est-à-dire de les *définir par récurrence* à partir de $s$, si bien que les trois axiomes de la section 1.1 déterminent toute l'arithmétique naturelle, c'est-à-dire la théorie opératoire des nombres entiers naturels.
Nous allons, en d'autres termes, "construire" rigoureusement l'addition et la multiplication des entiers naturels, et ultérieurement définir l'ordre naturel à partir de l'addition, comme nous avons défini la divisibilité à partir de la multiplication.
Cette approche jette une certaine lumière sur la théorie élémentaire des nombres et les relations entre les systèmes de nombres, et correspond à la philosophie générale qui consiste à "reconstruire" tous les objets mathématiques à partir des plus simples, les ensembles de nombres à partir de $\mathbb{N}$, les opérations à partir du successeur.
Elle servira aussi d'introduction naturelle à la théorie de la récursivité, pièce essentielle de la logique mathématique et fondement historique de l'informatique, pour les étudiant(e)s qui voudront s'y intéresser.
Nous commençons par l'addition.

**Définition 1.2.1.** L'*addition des entiers naturels* est l'unique application $+ : \mathbb{N}^2 \to \mathbb{N}$ possédant les propriétés suivantes, pour tous entiers naturels $m$ et $n$ :
i) $m + 0 = m$ (pour tout $m \in \mathbb{N}$, on pose $m + 0 := m$)
ii) $m+s(n) = s(m+n)$ (pour tous $m, n \in \mathbb{N}$, si $m+n$ est défini, on pose $m+(n+1) := (m + n) + 1$).

Il s'agit bien ici d'une définition par récurrence, dont le principe est appliqué comme suit : on *choisit* un entier naturel $m$ et on définit l'entier $m + n$ *pour tout entier naturel* $n$, en commençant par définir $m + 0$ et en utilisant la définition de $m + n$ pour concevoir celle de $m + s(n)$.
Par le théorème de récurrence 1.1.5, appliqué ici à l'ensemble $\mathbb{N}$, à l'élément $m$ et à la fonction $s$, il existe une unique application $g : \mathbb{N} \to \mathbb{N}$ telle que $g(0) = m$ et $g(s(n)) = s(g(n))$, et cette fonction est "l'addition de $n$ à $m$", autrement dit on a posé $m + n := g(n)$.
Ceci signifie que pour chaque entier naturel $m$, on définit une fonction différente, qui permet de définir $m + n$ pour tout $n \in \mathbb{N}$. Puisque la définition est posée pour tout entier naturel $m$ "fixé" (c'est-à-dire choisi à l'avance), l'expression $m + n$ est bien définie pour tous entiers naturels $m$ et $n$.

Il faut comprendre que les entiers $m$ et $n$ n'ont pas le même statut dans la définition : $m$ joue en quelque sorte le rôle de paramètre, tandis que la définition par récurrence porte sur $n$, une définition différente étant nécessaire pour chaque entier $m$.
Il faudra désormais revenir à cette *définition* dans toute utilisation de l'addition, par exemple dans les démonstrations, ce qui permettra de bien en comprendre le principe.
Les propriétés de l'addition, que nous avons auparavant considérées comme intuitives, vont en effet devenir des théorèmes, que nous allons devoir démontrer par récurrence. C'est tout l'intérêt de cette approche, qui nous permet de ramener la liste des propriétés intuitives de l'ensemble $\mathbb{N}$ à celles de l'axiomatique de Peano.
Notons que pour tout entier naturel $n$, l'expression $n+1$ est désormais définie à partir de la définition de $+$. En effet, par définition de la fonction successeur, de 0 et de 1, on a $1 = s(0)$; on en conclut alors que $n+1 = n+s(0) = s(n+0) = s(n)$. Si donc on définit 1 comme le successeur de 0, $n+1$ est le successeur de $n$.
Nous ne jouons pas ici sur les mots : dans les cours précédents, $n+1$ était *par définition* le successeur de $n$, au sens où nous avons défini de manière intuitive le successeur; à présent, l'expression reçoit son sens de la définition de l'addition.
Démontrons les propriétés élémentaires de celle-ci :

**Proposition 1.2.2.** *L'addition des entiers naturels possède les propriétés suivantes, pour tous entiers naturels $m, n$ et $p$ :*
*o)* $m+0 = m$
*i)* $(m+n)+p = m+(n+p)$ *(l'addition est dite "associative")*
*ii)* $m+n = n+m$ *(l'addition est dite "commutative").*

*Démonstration.* o) Cette propriété est vraie par définition.
i) Nous procédons par récurrence sur $p$, $m$ et $n$ étant donnés comme paramètres. Si $p = 0$, on a $(m+n)+p = (m+n)+0 = m+n$ (par définition) $= m+(n+0)$ (idem) $= m+(n+p)$, donc l'associativité est vérifiée pour $p = 0$. Supposons qu'elle le soit au rang $p$, c'est-à-dire que $(m+n)+p = m+(n+p)$ : on a $(m+n)+s(p) = s((m+n)+p))$ (par définition) $= s(m+(n+p))$ (par hypothèse de récurrence) $= m+s(n+p)$ (par définition) $= m+(n+s(p))$ (par définition), ce qui est l'associativité au rang $p+1$, donc la propriété est vérifiée pour tout $p \in \mathbb{N}$ par récurrence. Comme $m$ et $n$ sont arbitraires, elle est vérifiée pour tous $m, n, p \in \mathbb{N}$.
ii) Nous procédons par récurrence sur $n$, $m$ étant choisi comme paramètre. Si $n = 0$, on a $m+n = m+0 = m$ par définition : nous voulons montrer que $m = 0+m$, ce qui n'est pas dans la définition, donc nous introduisons un *second* argument par récurrence, à l'intérieur du premier, et portant cette fois-ci sur $m$. Si $m = 0$, on a $m = 0 = 0+0$ (par définition) $= 0+m$, donc la propriété est vérifiée pour $m = 0$. Supposons qu'elle le soit au rang $m$, c'est-à-dire que $m = 0+m$ : on a $s(m) = s(0+m)$ (par hypothèse de récurrence dans le second argument) $= 0+s(m)$ (par définition) donc la propriété est vraie pour tout $m$ par récurrence, ce qui clôt le second argument. On montrerait aussi par une autre récurrence auxiliaire que pour tout $m \in \mathbb{N}$, on a $m+1 = 1+m$. Revenant à notre argument principal, nous avons montré que $m+0 = m = 0+m$ pour tout $m \in \mathbb{N}$, donc la propriété (ii) est valide au rang $n = 0$. Supposons qu'elle le soit au rang $n$, c'est-à-dire que $m+n = n+m$ pour $m$ choisi d'avance; on obtient $m+(n+1) = m+s(n) = s(m+n)$

(par définition) $= s(n+m)$ (par hypothèse de récurrence) $= n+s(m)$ (par définition) $= n + (m + 1) = n + (1 + m)$ (par ce qui précède) $= (n + 1) + m$ (par (i)), donc $m + (n + 1) = (n + 1) + m$, ce qui est la propriété au rang $n + 1$, et par récurrence on conclut que (ii) est vraie pour tout $n \in \mathbb{N}$, et comme $m$ a été choisi de manière arbitraire, pour tous $m, n \in \mathbb{N}$. □

**Remarque 1.2.3.** Dans le principe de récurrence (axiome 1.1.3), on passe de l'étape $n$ à l'étape $s(n)$. Dans les raisonnements par récurrence introduits dans le premier cours, on passe du rang $n$ au rang $n + 1$. Ceci n'introduit pas d'ambiguïté puisque nous avons identifié $n + 1$ et $s(n)$ par définition de l'addition. Nous utilisons les deux notations selon le contexte.

La figure 1 représente l'étape de récurrence dans la définition de l'addition à partir de la fonction successeur.

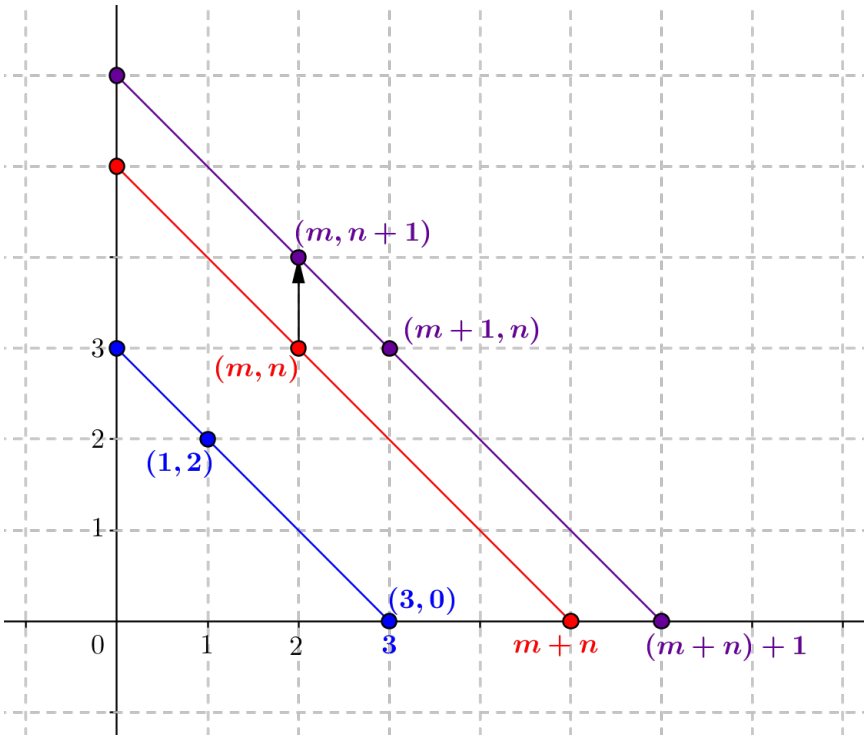



Figure 1: La somme de deux entiers naturels $m$ et $n$ est l'abscisse du point d'intersection de la "diagonale" sur laquelle se trouve le point $(m, n)$ avec l'axe des abscisses. La définition par récurrence de $m+(n+1)$ à partir de $m+n$ apparaît en passant verticalement du point $(m, n)$ au point $(m, n + 1)$, qui se trouve sur la diagonale "suivante". Les points $(m, n+1)$ et $(m+1, n)$ sont sur la même diagonale, illustrant que $(m + n) + 1 = (m + 1) + n$.

### 1.2.2 Définition de la multiplication

Nous poursuivons la "réduction" des opérations usuelles de l'ensemble $\mathbb{N}$ à la fonction successeur, en utilisant l'addition pour définir la multiplication, de nouveau par récurrence. Le procédé est analogue à ce que nous avons fait pour l'addition :

**Définition 1.2.4.** La *multiplication (des entiers naturels)* est l'unique application $\times : \mathbb{N}^2 \to \mathbb{N}$ possédant les propriétés suivantes, pour tous entiers naturels $m$ et $n$ :
i) $m \times 0 = 0$ (pour tout $m \in \mathbb{N}$, on pose $m \times 0 := 0$)
ii) $m \times s(n) = (m \times n) + m$ (pour tous $m, n \in \mathbb{N}$, si $m \times n$ est défini, on pose $m \times (n+1) := (m \times n) + m$).

Comme dans la définition de la somme, nous définissons le produit $m \times n$, par récurrence sur $n$, pour tout entier naturel $m$ séparément : il y a autant de définitions par récurrence que d'entiers $m \in \mathbb{N}$. Dans cette définition, nous utilisons d'ailleurs l'addition telle qu'elle est désormais définie par récurrence.
Nous noterons indifféremment $m \times n$, $m.n$ ou $mn$ le produit de deux entiers naturels $m$ et $n$. A partir de cette définition, les propriétés admises auparavant de manière intuitive pour la multiplication peuvent désormais être *démontrées* par récurrence.

**Proposition 1.2.5.** *La multiplication des entiers naturels possède les propriétés suivantes, pour tous entiers naturels $m, n$ et $p$ :*
*o)* $m.1 = m$
*i)* $(m+n).p = (m.p)+(n.p)$ *et* $p.(m+n) = p.m+p.n$ *(la multiplication est distributive sur l'addition)*
*ii)* $m.n = n.m$ *(la multiplication est commutative)*
*iii)* $(m.n).p = m.(n.p)$ *(la multiplication est associative).*

*Démonstration.* Nous démontrons ces propriétés en utilisant notamment les propriétés de l'addition démontrées dans la proposition 1.2.2.
o) On a $m.1 = m.s(0) = m.0 + m$ (par définition de $\times$) $= 0 + m$ (par définition de $\times$ à nouveau) $= m$, par les propriétés de l'addition.
i) Nous procédons par récurrence sur $p$. Si $p = 0$, on a $(m+n).0 = 0$ (par définition) $= (m.0) + (n.0)$ (par définition et par les propriétés de l'addition), donc la propriété est vérifiée au rang $p = 0$. Supposons qu'elle le soit au rang $p \geq 0$, c'est-à-dire que $(m+n).p = (m.p) + (n.p)$; on obtient $(m+n).s(p) = (m+n).p + (m+n)$ (par définition) $= (m.p) + (n.p) + m + n$ (par hypothèse de récurrence) $= (m.p+m) + (n.p+n)$ (par associativité de $+$) $= m.s(p) + n.s(p)$ (par définition), ce qui est la propriété au rang $s(p) = p+1$, et l'énoncé est démontré pour tout $p \in \mathbb{N}$ par récurrence. On démontrerait de même que $p.(m+n) = p.m + p.n$.
ii) Nous montrons d'abord que pour tout $n \in \mathbb{N}$, on a $0.n = 0$. Pour $n = 0$, c'est vrai par définition. Si c'est vrai au rang $n$, on a $0.s(n) = 0.n + 0$ (par définition) $= 0.0$ (par hypothèse de récurrence) $= 0$, donc la propriété est vraie au rang $s(n)$ et elle est donc vraie pour tout $n$ par récurrence. Nous montrons ensuite que pour tout $m \in \mathbb{N}$, on a $m.1 = m = 1.m$. Si $m = 0$, on a $m.1 = 0.1 = 1.0$ (par ce qui précède) $= 1.m$. Si la propriété est vérifiée pour $m$, on a $(m+1).1 = m.1 + 1.1$ (par (i)) $= m.1 + 1$ (par (o)) $= 1.m + 1$ (par hypothèse de récurrence) $= 1.(m+1)$, donc la propriété est vérifiée pour tout $m \in \mathbb{N}$ par récurrence. On montre alors la propriété générale par récurrence sur $n$, $m$ étant un entier naturel quelconque choisi. Si $n = 0$, on a $m.0 = 0.m = 0$ par ce qui précède, donc la propriété est vérifiée au rang $n = 0$. Supposons qu'elle le soit au rang $n \in \mathbb{N}$, c'est-à-dire que $m.n = n.m$ : on obtient $m.(n+1) = m.n + m$ (par définition) $= n.m + m$ (par hypothèse de récurrence) $= (n+1).m$ (par (o), (i) et ce qui précède) $= s(n).m$, donc la propriété est valide au rang $n+1$, et par récurrence elle l'est pour tout $n \in \mathbb{N}$, et donc pour

tous $m, n \in \mathbb{N}$, puisque $m$ a été choisi arbitrairement.
iii) Nous procédons à nouveau par récurrence sur $p$, $m$ et $n$ ayant été choisis arbitrairement. On a $(m.n).0 = 0 = m.0 = m.(n.0)$ par définition, donc la propriété est vérifiée pour $p = 0$. Si elle l'est pour $p$, autrement dit si on a $(m.n).p = m.(n.p)$, on obtient $(m.n).s(p) = (m.n).p + m.n$ (par définition) $= m.(n.p) + m.n$ (par hypothèse de récurrence) $= m.(n.p + n)$ (par (i) et (ii)) $= m.(n.s(p))$ (par définition); c'est la propriété au rang $p+1$, donc par récurrence la propriété est vérifiée pour tout $p \in \mathbb{N}$, et donc pour tous $m, n, p \in \mathbb{N}$. □

**Remarque 1.2.6.** Rappelons que lorsque nous démontrons par récurrence des propriétés dépendant de plusieurs entiers naturels, il arrive souvent que la récurrence porte sur l'un d'entre eux seulement, les autres étant "fixés", c'est-à-dire choisis arbitrairement mais déterminés. Par exemple, si la propriété $P(m, n, p)$ dépend de trois entiers, on veut montrer que l'ensemble des triplets $(m, n, p)$ pour lesquels $P(m, n, p)$ est vraie est l'ensemble $\mathbb{N}^3$ tout entier. Pour cela, on peut se ramener à montrer que si $m$ et $n$ quelconques sont donnés, $\{p \in \mathbb{N} : P(m, n, p)\}$ est $\mathbb{N}$ tout entier.

En outre, la multiplication possède la propriété dite "d'intégrité" suivante :

**Proposition 1.2.7.** *Si $m$ et $n$ sont deux entiers naturels tels que $m.n = 0$, alors $m = 0$ ou $n = 0$.*

*Démonstration.* Supposons que $m \neq 0$ et $n \neq 0$ : par la proposition 1.1.4, il existe $p, q \in \mathbb{N}$ tels que $m = p + 1$ et $n = q + 1$, d'où $m.n = (p + 1).(q + 1) = p.q + p + q + 1$, nombre différent de 0 par l'axiome 1.1.1, car successeur de $p.q + p + q$. Par contraposée, si $m.n = 0$, alors $m = 0$ ou $n = 0$. □

La figure 2 représente l'étape de récurrence dans la définition de la multiplication à partir de l'addition et du successeur.

## Exercices de la section

*Exercice* 1.2.8. i) (Subtil) Démontrer que l'addition, définie à partir du successeur, est l'addition dont on a admis l'existence et les propriétés de manière intuitive, autrement dit, qu'il n'existe qu'une seule application $A : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ qui possède les propriétés de la proposition 1.2.2.
ii) Compléter la démonstration de la proposition 1.2.2 en montrant que pour tout entier naturel $m$, on a $m + 1 = 1 + m$.
iii) Démontrer que pour tous entiers naturels $m, n$ et $p$, on a $m.(p+n) = m.p + m.n$, sans utiliser les clauses (ii) et (iii) de la proposition 1.2.5.
iv) Soit $f : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ une application telle que pour tous $m, n \in \mathbb{N}$, on a $f(m, 0) = 0$ et $f(m, n + 1) = f(m, n) + f(m)$. Montrer par récurrence que l'application $f$ est la multiplication.
v) Par définition, on a $2 = s(1)$, $3 = s(2)$, $4 = s(3)$, et ainsi de suite. Démontrer que $2 + 2 = 4$, $2 \times 2 = 4$, $2 + 3 = 5$ et $2 \times 3 = 6$.

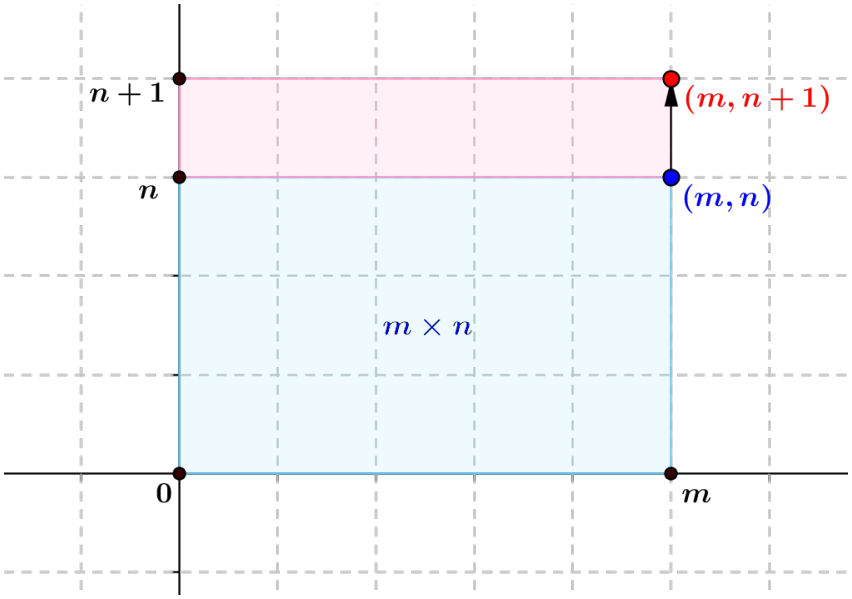



Figure 2: Le produit de deux entiers naturels $m$ et $n$ est l'aire du rectangle déterminé par le point $(m, n)$. La définition par récurrence de $m \times (n+1)$ à partir de $m \times n$ apparaît en passant verticalement du point $(m, n)$ au point $(m, n+1)$ : il faut ajouter à l'aire précédente celle d'un rectangle de côtés $m$ et 1, et donc d'aire $m = m \times 1$.

## 1.3 Les relations d'ordre naturel et de divisibilité

### 1.3.1 L'addition et l'ordre naturel

Dans le premier cours, nous avons adopté une compréhension intuitive de l'addition et de l'ordre naturel. En nous servant des relations intuitives entre les deux, nous pouvons désormais définir le second à partir de la première.
La propriété suivante de l'addition, appelée "simplifiabilité", est fondamentale et nous sera utile pour établir les propriétés de l'ordre naturel.

**Lemme 1.3.1.** *Soient $m, n$ et $p$ trois entiers naturels.*
*i) Si $m + n = m + p$, alors on a $n = p$ (l'addition dans $\mathbb{N}$ est "simplifiable").*
*ii) Si $m, n \in \mathbb{N}$ et $m + n = 0$, alors $m = n = 0$.*

*Démonstration.* i) On se donne $n$ et $p$ quelconques, et on procède par récurrence sur $m$. Supposons que $m = 0$ : si $m + n = m + p$, c'est que $n = 0 + n = 0 + p = p$ et la propriété est trivialement vraie dans ce cas. Supposons qu'elle le soit à un rang $m$, c'est-à-dire que l'énoncé "$\forall n, p \in \mathbb{N},\ m + n = m + p \Rightarrow n = p$" soit vrai; si maintenant $(m + 1) + n = (m + 1) + p$, par associativité de l'addition on a $m + (1 + n) = m + (1 + p)$ et par hypothèse de récurrence appliquée à $1 + n$ et $1 + p$, on a $1 + n = 1 + p$, soit $n + 1 = p + 1$ par commutativité de l'addition (1.2.2). Deux nombres ayant le même successeur sont égaux (par l'injectivité de $s$, axiome 1.1.2 de Peano), donc $n = p$, la propriété est vérifiée au rang $m + 1$, et par récurrence elle est vraie pour tout $m \in \mathbb{N}$, et donc pour tous $m, n, p \in \mathbb{N}$.
ii) Supposons par l'absurde que $m + n = 0$ mais que l'un des nombres $m$ ou $n$ n'est pas nul, par exemple $m$ (l'autre cas se traite de manière similaire par commutativité

de l'addition). Par la proposition 1.1.4, $m$ est le successeur d'un entier naturel $p$, c'est-à-dire $m = p + 1$. On obtient $0 = m + n = (p + 1) + n = (p + n) + 1$, par associativité et commutativité de l'addition; en particulier, 0 est le successeur de $p + n$, ce qui contredit l'axiome 1.1.1. Par *reductio ad absurdum*, on en conclut que $m = n = 0$. □

Souvenons-nous de la relation **intuitive** entre l'addition des entiers naturels et la relation d'inégalité large sur $\mathbb{N}$ : pour tous entiers naturels $m$ et $n$, on a $m \leq n$ si et seulement si il existe un entier naturel $p$ tel que $m + p = n$. Puisque nous avons *défini* l'addition à partir du successeur, nous allons désormais utiliser cette propriété pour *définir* la relation $\leq$ à partir de l'addition.

**Définition 1.3.2.** Si $m$ et $n$ sont deux entiers naturels, nous dirons que $m$ *est inférieur ou égal à* $n$, ce que nous notons $m \leq n$, si il existe un entier naturel $p$ tel que $m + p = n$. La relation binaire $(\mathbb{N}, \mathbb{N}, \leq)$ est appelée *ordre large* sur les entiers naturels.

**Remarque 1.3.3.** Insistons : ici, nous "oublions" volontairement l'approche intuitive de la relation $\leq$, de même que nous avons oublié dans la section précédente l'approche intuitive de l'addition et de la multiplication. Nous "reconstituons" tout à partir du successeur.

**Exemple 1.3.4.** Le nombre 2 est inférieur au nombre 5, parce qu'il existe un entier naturel $n = 3$, tel que $2 + 3 = 5$. En revanche, 2 n'est pas inférieur à 1, parce que pour aucun entier naturel $n$ on n'a $1 = 2 + n$ (sinon, par le lemme 1.3.1 on a aurait $0 = n + 1$, ce qui contredirait l'axiome 1.1.1).

On peut exprimer symboliquement cette définition en disant que la relation $\leq$ est définie comme la relation binaire sur $\mathbb{N}$, de graphe $R = \{(m, n) \in \mathbb{N}^2 : \exists p \in \mathbb{N},\ n = m + p\}$.
La relation $\leq$ étant à présent **définie** à partir de l'addition, ses propriétés élémentaires, admises de manière intuitive dans les premier cours, sont maintenant retrouvées comme conséquences des propriétés de l'addition :

**Proposition 1.3.5.** *Soient $m, n$ et $p$ des entiers naturels. On a les propriétés suivantes :*
*o) $0 \leq m$ (0 est le plus petit entier naturel)*
*i) $m \leq m$ (la relation $\leq$ est dite "réflexive")*
*ii) si $m \leq n$ et $n \leq p$, alors $m \leq p$ (la relation $\leq$ est dite "transitive")*
*iii) si $m \leq n$ et $n \leq m$, alors $m = n$ (la relation $\leq$ est dite "anti-symétrique")*
*iv) si $m \leq n$, alors $m + p \leq n + p$ (la relation $\leq$ est "compatible" à l'addition).*
*v) Si $m \leq n$, alors $m \times p \leq n \times p$ (la relation $\leq$ est "compatible" à la multiplication).*

*Démonstration.* o) Par la proposition 1.2.2, on a $0 + m = m$, donc par définition de $\leq$ on obtient $0 \leq m$.
i) Par définition de $+$, on a $m + 0 = m$, donc par définition de $\leq$ on a $m \leq m$.
ii) Si $m \leq n$ et $n \leq p$, par définition de $\leq$ il existe $q, r \in \mathbb{N}$ tels que $n = m + q$ et $p = n + r$, d'où $p = n + r = (m + q) + r = m + (q + r)$ par associativité de l'addition, et par définition de $\leq$, ceci signifie que $m \leq p$.

iii) Supposons que $m \leq n$ et $n \leq m$, c'est-à-dire qu'il existe $p, q \in \mathbb{N}$ tels que $n = m+p$ et $m = n+q$ : on obtient $n = m+p = (n+q)+p = n+(q+p)$ (par associativité de l'addition). Par le lemme 1.3.1 (clause (i)), on en déduit que $0 = p+q$, et par la clause (ii) du même lemme que $p = q = 0$, d'où $m = n+q = n+0 = n$.
iv) Supposons que $m \leq n$ : il existe $q \in \mathbb{N}$ tel que $n = m+q$, d'où $n+p = (m+q)+p = m+(q+p) = m+(p+q) = (m+p)+q$, c'est-à-dire $m+p \leq n+p$.
v) Si $m \leq n$, c'est qu'il existe un entier naturel $k$ tel que $m+k = n$ : on a alors $m.p + k.p = (m+k) \times p = n.p$ par les propriétés de la multiplication 1.2.5. Par définition de $\leq$, on a $m.p \leq n.p$. □

A partir de la relation d'ordre large $\leq$, nous pouvons désormais définir la relation d'ordre "strict" $<$, dit aussi "ordre linéaire", en posant, pour $m, n \in \mathbb{N}$, $m < n$ si et seulement $m \leq n$ et $m \neq n$. La propriété suivante est alors une conséquence directe de la définition de $\leq$ :

**Proposition 1.3.6.** *Pour tous entiers naturels $m$ et $n$, on a $m < n$ si et seulement si il existe $p \in \mathbb{N}^*$, tel que $n = m+p$.*

*Démonstration.* Supposons d'abord que $m < n$ : en particulier, on a $m \leq n$ donc il existe $p \in \mathbb{N}$, tel que $n = m+p$. Supposons par l'absurde que $p = 0$ : on a alors $n = m+p = m+0 = m$, ce qui contredit le fait que $m \neq n$; par *reductio ad absurdum*, on en déduit que $p \neq 0$. Réciproquement, supposons qu'il existe $p \neq 0$ tel que $n = m+p$ : on a donc $m \leq n$, et par la contraposée de la clause (i) du lemme 1.3.1, on a $m+0 \neq m+p$, c'est-à-dire $m \neq n$, d'où finalement $m < n$. □

**Exemple 1.3.7.** On a $11 < 17$, parce qu'il existe un entier naturel non nul $n = 6$ tel que $11+n = 17$. En revanche, on n'a pas $5 < 5$, parce qu'il n'existe pas d'entier naturel $n > 0$ tel que $5+n = 5$ (sinon, $n$ serait de la forme $m+1$ par la proposition 1.1.4, d'où $5 = 5+(m+1)$ et donc $0 = m+1$ par la proposition 1.3.1, ce qui contredirait à nouveau l'axiome 1.1.1).

La figure 3 représente les relations d'ordre large $\leq$ et d'ordre strict $<$ sur les entiers naturels, à partir de leur représentation sur les nombres réels.
Cette caractérisation "intrinsèque" de la relation $<$ à partir de l'addition ne mentionne plus la relation $\leq$ à partir de laquelle on l'a définie. Ceci signifie que nous aurions pu définir directement la relation $<$ à partir de $+$, et nous en aurions alors *déduit* que $m < n \Leftrightarrow (m \leq n \ \wedge \ m \neq n)$, ou nous aurions même pu définir $\leq$ à partir de $<$ en posant, pour tous entiers naturels $m, n$, $m \leq n$ si et seulement si $m < n$ ou $m = n$.
Les propriétés usuelles de $<$ sont reprises dans les exercices. L'important est ici de retenir la propriété de *trichotomie* de l'ordre linéaire :

**Proposition 1.3.8.** *Soient $m$ et $n$ deux entiers naturels. L'un des cas suivants est toujours vérifié, à l'exclusion des deux autres :*
*i) $m < n$*
*ii) $m = n$*
*iii) $m > n$.*

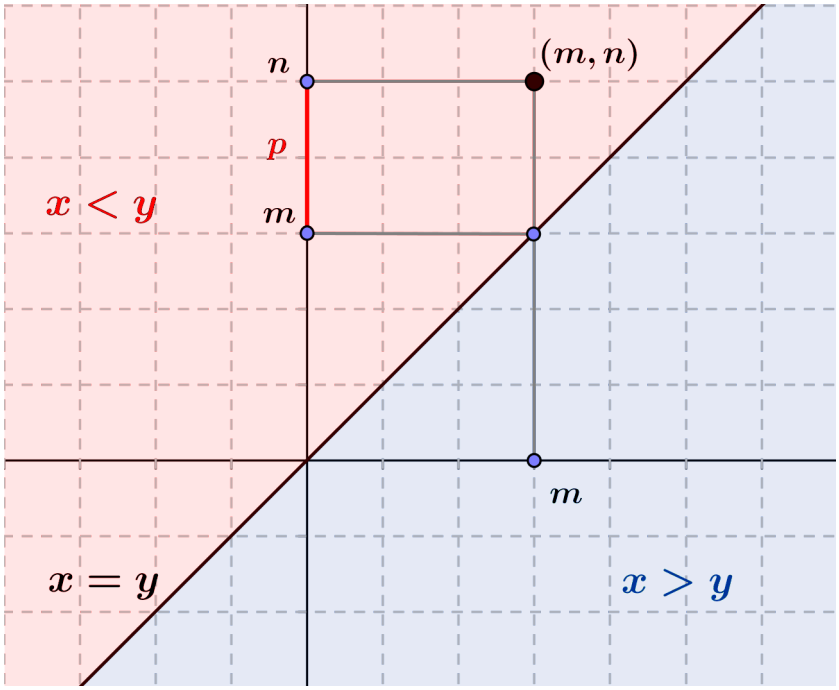



Figure 3: Les relations $\leq$ et $<$ sont représentées par différentes "régions" selon que les couples $(m, n)$ ont la propriété $m < n$, $m = n$ ou $m > n$. Le point $(m, n)$ est tel que $m \leq n$ : en projetant $m$ et $n$ sur l'axe des ordonnées, on observe qu'il existe $p$ tel que $n = m + p$. En fait, on a même $m < n$, si bien que $p > 0$.

*Démonstration.* Distinguons deux cas, selon qu'il existe $p \in \mathbb{N}$ tel que $n = m + p$ (c'est-à-dire $m \leq n$) ou non. Si un tel $p$ existe, alors soit $p \neq 0$ et $m < n$ par la proposition 1.3.6, soit $p = 0$ et alors $m = n$. Ces deux sous-cas sont évidemment mutuellement exclusifs. Dans le second cas, il n'existe pas d'entier naturel $p$ tel que $n = m + p$. Démontrons par récurrence sur $n$ que l'on a alors $n < m$; remarquons qu'on a toujours $n \neq m$, sinon on se trouve dans le premier cas. Si $n = 0$, alors on a $m = 0 + m = n + m$, d'où $n \leq m$, et donc $n < m$. Supposons que la propriété est vérifiée au rang $n$, c'est-à-dire que si on n'a pas $m \leq n$, alors $n < m$, et supposons qu'on n'a pas $m \leq n + 1$. En particulier, on n'a pas $m \leq n$, sinon il existerait $p \in \mathbb{N}$ tel que $n = m + p$, d'où $n + 1 = m + (p + 1)$, et on aurait $m \leq n + 1$. Par hypothèse de récurrence, on a donc $n < m$, donc il existe par la proposition 1.3.6 un entier naturel $p \neq 0$ tel que $n + p = m$. Par la proposition 1.1.4, $p$ est de la forme $s(q) = q + 1$, si bien que $n + p = n + (q + 1) = (n + 1) + q = m$, d'où $n + 1 \leq m$. Comme $m \neq n+1$, par le principe de récurrence, la propriété est démontrée au rang $n + 1$, si bien que le second cas est démontré et comme il est incompatible avec le premier, la démonstration est terminée. □

**Remarque 1.3.9.** Dans le second cas, on montre que si $m, n \in \mathbb{N}$ et $\neg(m \leq n)$, alors $n < m$. La démonstration se fait par récurrence, de la manière suivante : on considère $m$ comme "paramètre", c'est-à-dire un entier donné, et on montre que pour tout $n \in \mathbb{N}$, $\neg(m \leq n) \Rightarrow n < m$. L'utilisation du principe de récurrence consiste donc à démontrer que l'ensemble $\{n \in \mathbb{N} : \neg(m \leq n) \Rightarrow n < m\}$ est l'ensemble $\mathbb{N}$ tout entier.

### 1.3.2 Minimum et maximum

De la proposition 1.3.8, il découle que l'ordre $\leq$ est un ordre *total*, autrement dit que pour tous $m, n \in \mathbb{N}$, on a soit $m \leq n$, soit $n \leq m$.
En particulier, il existe toujours un *maximum* et un *minimum* pour deux tels éléments, au sens de la définition suivante :

**Définition 1.3.10.** Soient $n$ et $m$ deux entiers naturels.
i) Le *minimum de $n$ et $m$* est le plus petit des entiers $n$ et $m$, soit $n$ si $n \leq m$, ou $m$ si $m \leq n$. On le note $\min\{n, m\}$.
ii) Le *maximum de $n$ et $m$* est le plus grand des entiers $n$ et $m$, soit $m$ si $n \leq m$, ou $n$ si $m \leq n$. On le note $\max\{n, m\}$.

Les propriétés naturelles de min et de max sont les suivantes :

**Proposition 1.3.11.** *Si $m, n$ et $p$ sont trois entiers naturels, on a :*
*i)* $m = n$ *si et seulement si* $\min\{n, m\} = \max\{n, m\}$
*ii)* $m \leq n$ *si et seulement* $\min\{n, m\} = m$, *si et seulement* $\max\{n, m\} = n$
*iii)* $m + \min\{n, p\} = \min\{m + n, m + p\}$ *et* $m + \max\{n, p\} = \max\{m + n, m + p\}$
*iv)* $m \times \min\{n, p\} = \min\{m \times n, m \times p\}$ *et* $m \times \max\{n, p\} = \max\{m \times n, m \times p\}$.

*Démonstration.* La démonstration de (i) à (iii) est laissée en exercice à l'étudiant(e) (voir les exercices de la section). Démontrons (iv) en distinguant deux cas, selon que $n \leq p$ ou $p \leq n$. Si $n \leq p$, alors $\min\{n, p\} = n$, donc $m \times \min\{n, p\} = m \times n$; comme aussi $m \times n \leq m \times p$ par la proposition 1.3.5(v), on a $\min\{m \times n, m \times p\} = m \times n$, d'où la première égalité dans ce cas. Si $p \neq n$, en échangeant les rôles de $n$ et $p$ dans le premier cas, on obtient aussi la première égalité. La seconde égalité se démontre de manière parfaitement analogue. □

**Exemple 1.3.12.** Le minimum de 15 et 9 est 9, puisque $9 < 15$ et pour la même raison, le maximum de 9 et 15 est 15. On vérifie bien qu'on a $\min\{20, 31\} = 11 + \min\{9, 15\} = 20$, et qu'on a $\max\{63, 105\} = \max\{9.7, 15.7\} = 7 \times \max\{9, 15\} = 7.15 = 105$.

### 1.3.3 La multiplication et la divisibilité

Notre définition de la relation d'ordre large $\leq$ à partir de l'addition était l'analogie parfaite de celle que nous avons donnée dès le premier cours, de la relation de *divisibilité* $|$ à partir de la multiplication. Nous avons en effet décrété que pour tous $m, n \in \mathbb{N}$, $m$ divise $n$ si et seulement si il existe $d \in \mathbb{N}$ tel que $n = m.d$, symboliquement : $m|n \Leftrightarrow \exists d \in \mathbb{N},\ m.d = n$.
Cette définition étant parfaitement rigoureuse, elle s'intègre à notre description de $\mathbb{N}$ à partir de l'arithmétique de Peano. L'arithmétique "naturelle", à proprement parler, est l'étude de la relation de divisibilité dans l'ensemble $\mathbb{N}$, que nous entreprendrons dans la suite du chapitre et poursuivrons par l'arithmétique élémentaire dans l'ensemble $\mathbb{Z}$ au chapitre suivant.
Pour l'heure, nous énonçons les propriétés élémentaires de $|$, analogues à celles de $\leq$, qui proviennent directement des propriétés de $\times$.

**Définition 1.3.13.** Si $m$ et $n$ sont deux entiers naturels tels que $m|n$, on dit que $n$ est un *multiple de* $n$ et que $m$ est un *diviseur de* $n$.

**Exemple 1.3.14.** Le nombre 1031 est un multiple de 7 et un multiple de 11, puisqu'il existe $d = 143$ tel que $1031 = d \times 7$, et $k = 91$ tel que $1031 = k \times 11$. En revanche, le nombre 14 n'est pas un diviseur de 128, car sinon il existerait $k \in \mathbb{N}$ tel que $14.k = 128$ : on aurait nécessairement $k \leq 9$ (puisque si $k > 9$, on a $k \geq 10$, donc $14.k \geq 140 > 128$ par la proposition 1.3.5(v)) mais pour $k \leq 9$ on a $14.k \leq 126$ par la même proposition.

**Proposition 1.3.15.** *Soient $m, n, p \in \mathbb{N}$. On a les propriétés suivantes :*
*o) $1|m$ (1 est le "diviseur universel") et $m|0$ (0 est le "multiple universel")*
*i) $m|m$ (la relation $|$ est réflexive)*
*ii) si $m|n$ et $n|p$, alors $m|p$ (la relation $|$ est transitive)*
*iii) si $m|n$ et $n|m$, alors $m = n$ (la relation $|$ est anti-symétrique).*

*Démonstration.* Laissée comme un exercice pour l'étudiant(e) (imiter la preuve de la proposition analogue pour $\leq$). □

Notons pour terminer les propriétés suivantes de "compatibilité de l'ordre strict à la multiplication", la seconde étant analogue à 1.2.7.

**Proposition 1.3.16.** *Pour tous entiers naturels $m, n$ et $p$ :*
*i) si $m < n$ et $p \neq 0$, on a $m.p < n.p$*
*ii) si $m.p = n.p$ et $p > 0$, on a $m = n$.*

*Démonstration.* i) La démonstration est laissée en exercice à partir de la proposition 1.3.5.
ii) Supposons que $m \neq n$ : par la proposition 1.3.8, on a $m < n$ ou $n < m$; par (ii), dans les deux cas on a $m.p \neq n.p$, d'où le résultat par contraposée. □

## Exercices de la section

*Exercice* 1.3.17. i) Montrer que pour tous entiers naturels $m$ et $n$, on a $m < n$ si et seulement si il existe $p \in \mathbb{N}$ tel que $n = m + p + 1$. En déduire que $m < n$ si et seulement si $m + 1 \leq n$.
ii) Démontrer les propriétés suivantes :
- pour tout $m \in \mathbb{N}$, on a $0 < m + 1$
- pour tout $m \in \mathbb{N}$, on n'a jamais $m < m$
- pour tous $m, n, p \in \mathbb{N}$ tels que $m < n$ et $n < p$, on a $m < p$
- pour tous $m, n, p \in \mathbb{N}$ tels que $m < n$, on a $m + p < n + p$.

iii) Démontrer la proposition 1.3.11.
iv) Démontrer les propriétés de la proposition 1.3.15.
v) Montrer que si $n, m \in \mathbb{N}$, $m \neq 0$ et $n|m$, alors $n \leq m$.
vi) Démontrer la clause (i) de la proposition 1.3.16.
vii) Démontrer que pour tout entier naturel $n$, on a $n < s(n)$. En déduire que $2 < 4$. Indication : par définition, $2 = s(1)$.

*Problème* 1.3.18 (Facultatif, plus difficile). Le sujet de ce problème est de donner une définition rigoureuse de $\leq$ (ou de $<$) qui ne dépend pas de l'addition; il s'agit de la définition de Bertrand Russell dans *Introduction to mathematical philosophy*. Nous allons pour cela *caractériser* l'ordre $\leq$ tel qu'il est défini ici par cette propriété alternative.
Une propriété $P$ des entiers naturels est dit *héréditaire* si elle est vraie pour un entier naturel $n+1$ (c'est-à-dire $s(n)$) dès qu'elle l'est pour un entier naturel $n$, autrement dit, si l'énoncé "$\forall n,\ P(n) \Rightarrow P(n+1)$" est vrai. Nous proposons alors de démontrer que $m \leq n$ si et seulement si $n$ possède toute propriété héréditaire que possède $m$.
i) Soit $m \in \mathbb{N}$. Montrer que la propriété $P(k)$ définie par "$\exists p \in \mathbb{N},\ m+p=k$", où $m$ est considéré comme un paramètre, est héréditaire.
ii) En déduire que si $n \in \mathbb{N}$ possède toute propriété héréditaire que possède $m$, alors $m \leq n$.
iii) Supposons que $m \leq n$, et soit $p \in \mathbb{N}$ tel que $m+p=n$. Montrer par récurrence sur $p$ que si $P$ est une propriété héréditaire que possède $m$, alors $n$ possède cette propriété. Conclure.
iv) Montrer que $m < n$ si et seulement si $s(n)$ possède toute propriété héréditaire que possède $m$.

## 1.4 Divisibilité et division euclidienne

A l'école primaire, nous apprenons à diviser un entier naturel $a$ par un autre entier naturel $b$ non nul : le résultat est donné en général sous la forme d'un quotient $q$ et d'un reste $r$ sous la forme $a = b \times q + r$ avec $r < b$, et $r$ est nul *exactement lorsque $a$ est divisible par $b$*. En revanche, lorsque $r \neq 0$ la division euclidienne ne donne qu'une *approximation* de la division de $a$ par $b$.
L'interprétation intuitive de la division euclidienne, sur le plan des quantités, est la suivante : combien de fois $b$ est-il "contenu" dans $a$ ? Ou encore : étant donnée une collection de $a$ objets, quel est le nombre maximal $q$ de "paquets" de $b$ objets qu'on peut faire avec ceux-ci ? Ce nombre est maximal exactement lorsque, une fois les "paquets" rassemblés, les objets restant éventuellement ne permettent pas de former un nouveau paquet, leur nombre $r$ étant donc strictement inférieur à $b$.
Nous reconstruisons ici la théorie de la division euclidienne en utilisant nos nouveaux concepts mathématiques et les axiomes du successeur dans $\mathbb{N}$, et nous lui donnons ainsi un fondement numérique solide qui ne dépend plus de l'intuition des ensembles $\mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$ comme dans le cours n° 1.
Nous pouvons traduire l'interprétation précédente sur le plan de la théorie des ensembles finis comme suit : combien d'ensembles deux-à-deux disjoints de $b$ éléments pouvons-nous former avec un ensemble de $a$ éléments ? Si $a$ est un multiple de $b$, disons $a = b.d$, alors la réponse est $d$, bien sûr, mais en général $a$ n'est pas divisible par $b$, donc il nous faut obtenir la "meilleure approximation".
Nous aurons pour ceci besoin de résultats auxiliaires sur le "plus grand élément" et le "plus petit élément" de certains sous-ensembles de $\mathbb{N}$ (on pourra se reporter au cours n° 2 pour la théorie des ensembles finis et de leur cardinal).

**Lemme 1.4.1.** *Tout sous-ensemble fini $S$ non vide de $\mathbb{N}$ possède un plus grand élément, autrement dit il existe $n \in S$ tel que pour tout $m \in S$, on ait $m \leq n$.*

*Démonstration.* On procède par récurrence sur le cardinal $k$ de $S$. Si $k = 1$, alors $S$ ne possède qu'un élément $n$, qui est nécessairement le plus grand élément de $S$. Supposons que la propriété est vérifiée pour les sous-ensembles finis de cardinal $k > 1$, et que $|S| = k+1$. Soit $i \in S$ un élément quelconque : l'ensemble $S - \{i\}$ est fini et possède $k$ éléments (Cours n° 3, chapitre 2), donc par hypothèse de récurrence il possède un plus grand élément, appelons-le $m$. Soit alors $n$ le plus grand des deux nombres $i$ et $m$, par la proposition 1.3.8, et soit $j \in S$ : si $j = i$, alors on a $j \leq n$, tandis que si $j \neq i$, par définition de $m$ on a $j \leq m \leq n$. Il s'ensuit que $n$ est le plus grand élément de $S$, et le lemme est démontré par récurrence. □

**Exemple 1.4.2.** L'ensemble $2\mathbb{N}$ des entiers naturels pairs (c'est-à-dire multiples de 2) est infini, donc il ne possède pas de plus grand élément (par contraposée du lemme 1.4.1). En effet, si $n \in 2\mathbb{N}$, $n$ est de la forme $2.m$ pour $m \in \mathbb{N}$, et on a $n = 2.m. < 2.(m+1) \in 2\mathbb{N}$.

**Proposition 1.4.3.** *Tout sous-ensemble non vide $S$ de $\mathbb{N}$ possède un plus petit élément, autrement dit il existe $n \in S$ tel que pour tout $m \in S$, on a $n \leq m$.*

*Démonstration.* Distinguons deux cas. Dans le premier, si $0 \in S$ alors 0 est évidemment le plus petit élément de $S$. Dans le second, on suppose que $0 \notin S$, et on considère alors l'ensemble $X$ de tous les entiers naturels qui sont strictement plus petits que *tous* les éléments de $S$, c'est-à-dire $X = \{i \in \mathbb{N} : \forall m \in S,\ i < m\}$. Par hypothèse, $X$ n'est pas vide, puisque $0 \in X$. Comme $S$ n'est pas vide non plus, il existe $a \in S$, si bien que $X \subseteq [[0, a]] = \{n \in \mathbb{N} : n \leq a\}$, donc $X$ est fini comme sous-ensemble d'un ensemble fini (Cours n° 3, chapitre 2). Par le lemme 1.4.1, $X$ possède un plus grand élément, notons-le $k$. Par définition de $X$ et de $k$, pour tout $m \in S$ on a donc $k < m$, soit, par l'exercice 1.3.17(i), $k+1 \leq m$. Comme $k+1 \in S$, il s'ensuit que $k+1$ est le plus petit élément de $S$. □

**Remarque 1.4.4.** Cette propriété de l'ordre naturel sur $\mathbb{N}$ concerne *tous* les sous-ensembles de $\mathbb{N}$, et est à la base de la représentation de $\mathbb{N}$, avec la relation $<$, comme un *ordinal*, c'est-à-dire la version formelle d'un nombre infini conçu comme un "type d'ordre". La proposition 1.4.3 est en fait équivalente au principe de récurrence (voir les exercices).

**Théorème 1.4.5** (Division euclidienne)**.** *Si $a$ et $b$ sont deux entiers naturels tels que $b \neq 0$, alors il existe deux entiers naturels $q$ et $r$ uniques, tels que $a = b.q + r$ et $r < b$. Les nombres $q$ et $r$ sont appelés respectivement le* quotient *et le* reste *de la* division euclidienne *de $a$ par $b$.*

*Démonstration.* Nous démontrons d'abord l'existence de $q$ et de $r$. Soit $b\mathbb{N}$ l'ensemble des multiples de $b$, explicitement $b\mathbb{N} = \{b.d : d \in \mathbb{N}\}$, image de l'application $M_b : \mathbb{N} \to \mathbb{N}$, $d \mapsto b.d$ de "multiplication par $b$". L'ensemble $[[0, a]] = \{n \in \mathbb{N} : n \leq a\}$ est fini (voir le cours n° 3, chapitre 2), donc le sous-ensemble $b\mathbb{N} \cap [[0, a]]$ est fini également (idem); n'étant pas vide puisqu'il contient $0 = b.0$, il possède alors un plus grand élément $k$ par le lemme 1.4.1, qui est de la forme $b.q$. Par définition

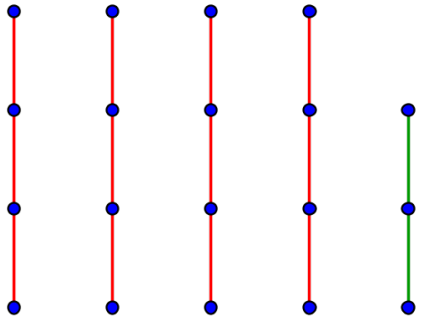


Figure 4: Division euclidienne de 19 par 4 : on a $19 = 4 \times 4 + 3$, et $3 < 4$, donc 4 est le quotient, et 3 est le reste, et 4 ne divise pas 19. Sur la figure, on peut faire 4 "paquets" (quotient) de 4 points, et il reste un paquet de 3 points.

de $k$, on a $b.q \leq a$, donc par définition de $\leq$ il existe un entier naturel $r$ tel que $a = b.q + r$. Supposons par l'absurde que l'on a $r \geq b$ : par les propriétés de $\leq$ (proposition 1.3.5(iv)), on obtient $a = b.q + r \geq b.q + b = b.(q + 1)$, ce qui entraîne que $b.(q + 1) \in b\mathbb{N} \cap [[0, a]]$; comme $k = bq < b(q + 1) = bq + b$, ceci contredit la définition de $k$, donc par *reductio ad absurdum*, on a $r < b$ et l'existence de $q$ et de $r$ est démontrée. En ce qui concerne leur unicité, supposons que $q', r' \in \mathbb{N}$ sont tels que $a = b.q' + r'$ avec $r' < b$; on obtient $b.q' \leq a < b.q' + b = b.(q' + 1)$, donc $q'$ est le plus grand élément de $b\mathbb{N} \cap [[0, a]]$, soit $q = q'$, et $b.q + r = b.q + r'$; par la proposition 1.3.1 (clause (i)), on obtient $r = r'$, et le théorème est démontré. □

**Remarque 1.4.6.** Dans la démonstration de cet énoncé dans le cours n° 1, nous avons utilisé les propriétés intuitives de la soustraction dans l'ensemble $\mathbb{Z}$ et de la valeur absolue dans l'ensemble $\mathbb{R}$. Ici la propriété de simplifiabilité de l'addition dans $\mathbb{N}$ permet de se passer de la soustraction, tandis que l'usage du plus grand élément d'un ensemble fini permet de se passer de la valeur absolue.

La figure 4 représente représente une division euclidienne par "paquets".

**Définition 1.4.7.** Si $a$ et $b$ sont deux entiers naturels avec $b > 0$, on dit que $a$ est le *dividende* et $b$ le *diviseur* de la division euclidienne $a = b.q + r$.

**Exemple 1.4.8.** On a $527 = 48 \times 10 + 47$; comme $47 < 48$, 10 est le quotient et 47 est le reste, de la division euclidienne de 527 (dividende) par 48 (diviseur).

**Corollaire 1.4.9.** *Si $a$ et $b$ sont deux entiers naturels, avec $b \neq 0$, alors $b$ divise $a$ si et seulement si le reste de la division euclidienne de $a$ par $b$ est 0.*

*Démonstration.* Si $b|a$, alors il existe par définition $d \in \mathbb{N}$ tel que $a = b.d = b.d + 0$, donc par unicité du quotient et du reste dans la division euclidienne de $a$ par $b$, $d$ est le quotient, et 0 est le reste, de cette division. Inversement, écrivons la division euclidienne de $a$ par $b$ sous la forme $a = b.q + r$, avec $r < b$ : si $r = 0$, on a $a = b.q$, donc $b|a$. □

**Remarque 1.4.10.** Ce corollaire peut paraître évident, à cause de l'intuition de ce que signifie la division euclidienne, mais il est nécessaire de le démontrer.

Un entier naturel $d$ tel que $d$ divise $n$ est appelé un *diviseur* de $n$, et $n$ est alors appelé un *multiple* de $d$.

### Exercices de la section

*Exercice* 1.4.11. i) Démontrer par l'absurde le principe de récurrence à partir des deux premiers axiomes de Peano et de la proposition 1.4.3. Indication : si $S \subseteq \mathbb{N}$ est un sous-ensemble tel que $0 \in S$ et $s(n) \in S$ dès que $n \in S$, supposer que $S \neq \mathbb{N}$, et considérer le plus petit élément du sous-ensemble non vide $\mathbb{N} - S$ de $\mathbb{N}$.
ii) Effectuer la division euclidienne de 247 par 53.
iii) Quel est le reste dans la division euclidienne de 114 par 3 ?
iv) Soient $a, b \in \mathbb{N}$, avec $b > 0$. Supposons que $a < b$; quels sont le quotient et le reste de la division euclidienne de $a$ par $b$ ?
v) Soient $a, b \in \mathbb{N}$, avec $a > 0$ et $b > 1$. Montrer qu'il existe un unique entier naturel $n$ tel que $b^n \leq a < b^{n+1}$.

## 1.5 Les nombres premiers

Un nombre entier naturel différent de 0 et de 1 est dit *premier* si il ne peut pas être "décomposé" en un produit de deux nombres différents de 1. Plus précisément :

**Définition 1.5.1.** i) Un entier naturel non nul $n$ différent de 1 est *premier* si pour tout entiers naturels non nuls $m, p$ tels que $n = mp$, on a $m = 1$ ou $p = 1$.
ii) Si $n$ est un entier naturel, un nombre premier $p$ tel que $p$ divise $n$ est appelé un *facteur premier* de $n$.

**Remarque 1.5.2.** Par la proposition 1.2.7, la propriété est équivalente à ce que pour tous entiers naturels $m, p$ tels que $n = mp$, on a $n = m$ ou $n = p$. En effet, si $n$ est premier et $n = mp$, alors clairement soit $n = p$ (cas où $m = 1$) soit $n = m$ (cas où $p = 1$). Inversement, si cette propriété est vérifiée et $n = mp$, supposons que $n = m$ : on a $n = m.1 = mp$; par la proposition 1.3.16(ii), on a $p = 1$; de même, si $n = p$ on a $m = 1$, et $n$ est premier.

**Exemple 1.5.3.** i) Les nombres $2, 3, 5, 7$ sont premiers. Par exemple, supposons que $2 = mn$ : on a alors $m, n \neq 0$ et $m, n \leq 2$, donc soit $m = 1$, soit $m = 2$ et alors $n = 1$ (1.3.16(ii) à nouveau), donc 2 est premier. Pour montrer que 3 est premier, on peut utiliser une division euclidienne : les seuls diviseurs possibles de 3 sont 1, 2 et 3, et pour exclure 2 on peut écrire $3 = 2.1 + 1$, division de 3 par 2, d'où $2 \nmid 3$ (2 ne divise pas 3) par le corollaire 1.4.9, et finalement 3 est premier. La primalité de 5 et 7 est laissée en exercice.
ii) Les facteurs premiers de 12 sont 2 et 3. les facteurs premiers de 45 sont 3 et 5. Les facteurs premiers de 77 sont 7 et 11.

**Remarque 1.5.4.** Il est important de comprendre ici qu'en toute rigueur il faut démontrer que les nombres $2, 3, 5, 7, \ldots$ sont premiers, et que pour cela il faut revenir à la définition même de ces nombres et des opérations d'addition et de multiplication.

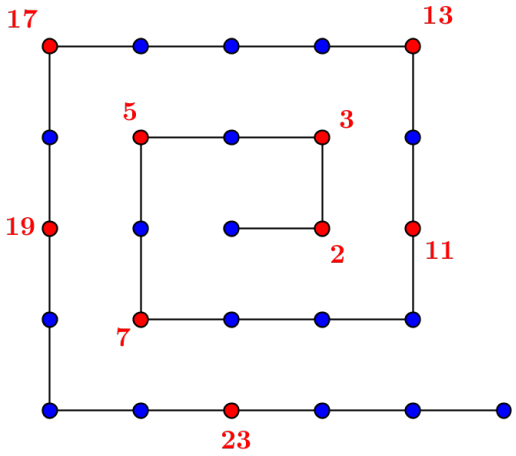



Figure 5: Quelques nombres premiers, tels qu'ils se répartissent sur la "spirale d'Ulam".

La figure 5 donne une représentation classique de quelques nombres premiers.
On formule aussi souvent la définition d'un nombre premier comme un entier naturel ayant exactement 2 diviseurs, 1 et lui-même. Avant de donner les premiers exemples, notons une propriété essentielle de la "décomposition" d'un nombre en un produit de deux facteurs.

**Lemme 1.5.5.** *Supposons que $n, k$ et $l$ sont trois entiers naturels tels que $n > 1$, $n = kl$ et $1 < k < n$ : alors, on a aussi $1 < l < n$.*

*Démonstration.* Comme $n \neq 0$, on a aussi $l \neq 0$ (sinon $n = kl = k.0 = 0$). Si $l = 1$, alors on a $n = kl = k.1 = k$, ce qui contredit $k < n$ : on en déduit que $l > 1$. Or, par l'exercice 1.3.17(v), comme $l|n$ et $n \neq 0$, on a $l \leq n$ et si $l = n$, on a $n = kl = kn > n$ par la proposition 1.3.16, ce qui est absurde; on en déduit que $l < n$. □

La première chose que nous allons établir à propos des nombres premiers, c'est qu'il sont en nombre infini. C'est possible grâce à la théorie des ensembles infinis développée dans le cours précédent (cours n° 2).

**Lemme 1.5.6.** *Pour tout entier naturel $n \geq 2$, il existe un nombre premier $p$ tel que $p|n$ (tout nombre entier naturel $\geq 2$ possède un facteur premier).*

*Démonstration.* Nous procédons par récurrence sur $n$. Si $n = 0$, il n'y a rien à démontrer. Supposons que $n > 0$ et que la propriété est vérifiée pour tout $m < n$. Soit $n$ est premier, auquel cas $n|n$ et $n$ est un facteur premier de lui-même, soit $n$ n'est pas premier, auquel cas il existe deux entiers naturels $k, l < n$ tels que $1 < k, l$ et $n = kl$; dans ce cas, par hypothèse de récurrence appliquée à $k$ disons, il existe un nombre premier $p$ tel que $p|k$, donc aussi $p|n$. Par le principe de récurrence, la démonstration est complète. □

**Remarque 1.5.7.** On utilise dans cette démonstration une variante du raisonnement par récurrence : pour démontrer une propriété $P(n)$ qui dépend d'un entier $n$, (ici, $P(n)$ est la propriété "si $n \geq 2$, alors il existe un nombre premier $p$ tel que

$p|n$"), on démontre en fait la propriété $Q(n)$ qui est "pour tout entier $k \leq n$, $P(k)$". En effet, si on écrit $n = m + 1$ à l'étape de récurrence, on a besoin de pouvoir appliquer l'hypothèse de récurrence à tous les entiers inférieurs à l'entier $m$, et pas seulement à $m$. On établit donc en fait le lemme sous la forme de l'énoncé $\forall n\ Q(n)$, qui est équivalent à $\forall n\ P(n)$.

Si $a, b \in \mathbb{N}$ et si $a \leq b$, par définition il existe $x \in \mathbb{N}$ tel que $a + x = b$. Notons dans ce cas $b - a$ le nombre $x$ : il s'agit ici d'une *notation*, car l'opération de soustraction ne peut être définie dans tous les cas.

**Lemme 1.5.8.** *Soient $a, b, c \in \mathbb{N}$, tels que $a \leq b$ et $c \geq 2$. Si $c$ divise $a$ et $b$, alors $c$ divise $b - a$.*

*Démonstration.* Ecrivons que $c$ divise $a$ et $b$ : il existe des entiers naturels $x$ et $y$ tels que $a = cx$ et $b = cy$, d'où $cy = b = a + (b - a) = cx + (b - a)$. Effectuons la division euclidienne de $b - a$ par $c$ : il existe $q, r \in \mathbb{N}$ uniques tels que $b - a = cq + r$ et $r < c$. Il vient $cx + (b - a) = cx + cq + r = c(x + q) + r = cy$. Par unicité du reste de la division euclidienne de $b$ par $c$, on en déduit que $r = 0$, si bien que $c|b - a$ par le corollaire 1.4.9. □

Pour démontrer le théorème fondamental suivant, rappelons (voir le Chapitre 2 du cours n° 2) qu'une application de la forme $a : [[1, n]] \to E$ est appelée un *$n$-uplet*, et qu'on écrit plutôt $a_i$ pour $a(i)$, de sorte qu'on décrit $a$ comme une "suite finie" $(a_1, \ldots, a_n)$ d'éléments de $E$. Précisons également ce que nous entendons par le produit de $n$ entiers naturels $k_1, \ldots, k_n$. Un tel produit, noté par exemple $k_1 \ldots k_n$, possède une signification intuitive claire, mais on le définit rigoureusement par récurrence sur $n \geq 2$. Si $n = 2$, le produit de deux entiers $k_1$ et $k_2$ est par définition le résultat de leur multiplication $k_1 \times k_2$, et si on sait définir le produit de $n-1$ entiers pour $n-1 \geq 2$, on *définit* le produit $k_1 \ldots k_n$ de $n$ entiers $k_1, \ldots, k_n$ (pas nécessairement distincts), comme le produit de $k_1 \ldots k_{n-1}$ et de $k_n$, soit $(k_1 \ldots k_{n-1}) \times k_n$.

**Lemme 1.5.9.** *Supposons que $n \geq 1$ et que $k_1, \ldots, k_n$ sont $n$ entiers naturels (c'est-à-dire que $(k_1, \ldots, k_n)$ est un $n$-uplet d'entiers naturels). Pour tout $i \in \{1, \ldots, n\}$, $k_i$ divise le produit $k_1 \ldots k_n$.*

*Démonstration.* On raisonne par récurrence sur $n$. Si $n = 0$, alors par convention ou définition le produit $k_1 \ldots k_n$ est "vide" et vaut 1 et comme $[[1, n]]$ est vide, la propriété est vérifiée. On peut sinon commencer la récurrence au rang $n = 1$ : le produit vaut $k_1$ et évidemment $k_1|k_1$. Supposons que la propriété est vérifiée au rang $n$, et que $k_1, \ldots, k_{n+1}$ sont $n + 1$ entiers naturels : par définition, on a $k_1 \ldots k_{n+1} = (k_1 \ldots k_n) \times k_{n+1}$. Soit alors $i \in [[1, n + 1]]$ : si $i \in [[1, n]]$, alors par hypothèse de récurrence on a $k_i|k_1 \ldots k_n$, donc $k_i|k_1 \ldots k_{n+1}$, tandis que si $i = n+1$, par définition on a $k_{n+1}|k_1 \ldots k_{n+1}$ et la propriété est démontrée au rang $n + 1$, et donc pour tout entier naturel $n$ par récurrence. □

**Théorème 1.5.10** (Euclide)**.** *L'ensemble des nombres premiers est infini.*

*Démonstration.* Supposons par l'absurde que l'ensemble $P$ des nombres premiers est fini : comme il n'est pas vide, il existe un entier naturel $n \geq 1$ et des nombres premiers $p_1, \ldots, p_n$ tels que $P = \{p_1, \ldots, p_n\}$ (autrement dit, il existe $n \in \mathbb{N}^*$ et une bijection de $[[1, n]]$ sur $P$). Considérons le nombre $m = p_1 \ldots p_n + 1$ (où $p_1 \ldots p_n$ désigne le produit des nombres $p_1, \ldots, p_n$) : comme $m \geq 2$, par le lemme 1.5.6 il existe au moins un facteur premier, disons $q$, de $m$, qui doit donc être un élément de $P$, c'est-à-dire qu'il existe $i \in \{1, \ldots, n\}$ tel que $q = p_i$. En particulier, par le lemme 1.5.9 on a $q | p_1 \ldots p_n$, donc aussi $q | m - p_1 \ldots p_n = 1$ par le lemme 1.5.8, ce qui est impossible car $1 < q$. Par *reductio ad absurdum*, on en conclut que l'ensemble des nombres premiers est infini. □

Pour pouvoir déterminer si un nombre entier naturel $n \geq 2$ donné est premier, il suffit de "tester" sa divisibilité par tous les nombres premiers qui lui sont strictement inférieurs. En effet, s'il existe un nombre premier $p < n$ tel que $p | n$, alors $n$ n'est pas premier, car il s'écrit sous la forme $n = pm$, avec $p, m \neq 1, n$. Inversement, si $n$ n'est pas premier, alors il existe par le lemme 1.5.6 un diviseur premier de $n$, qui lui est nécessairement strictement inférieur. Par conséquent, on peut énoncer la

**Proposition 1.5.11.** *Un entier naturel $n \geq 2$ est premier si et seulement si il ne possède pas de facteur premier $p < n$.*

On peut significativement simplifier ce "test de primalité" élémentaire en utilisant le résultat suivant, qui nous garantit qu'il suffit de tester seulement "quelques" nombres premiers.

**Proposition 1.5.12.** *Si $n$ est un entier naturel supérieur à 2, alors $n$ est premier si et seulement si il ne possède pas de facteur premier $p$ tel que $p^2 \leq n$ (autrement dit, tel que $p \leq \sqrt{n}$ dans $\mathbb{R}$).*

*Démonstration.* Evidemment, si $n$ est premier il ne possède pas de facteur premier $p$ tel que $p^2 \leq n$, sinon on aurait $p < p^2 \leq n$, ce qui contredit la proposition 1.5.11. Inversement, montrons que si $n$ n'est pas premier, alors il possède un facteur premier $p$ tel que $p^2 \leq n$. Par définition, il existe $m, k \in \mathbb{N}$ tels que $n = mk$ et $m, k \neq 1, n$; par le lemme 1.5.5, on a $1 < m, k < n$. Par le lemme 1.5.6, chacun des nombres $m$ et $k$ possède un facteur premier, disons $p$ pour $m$ et $q$ pour $k$, de sorte que $p \leq m$ et $q \leq k$, et $p$ et $q$ sont des facteurs premiers de $n$. Si on avait à la fois $m^2 > n$ et $k^2 > n$ (c'est-à-dire $m \geq \sqrt{n}$ et $k \geq \sqrt{n}$), alors on aurait $(mk)^2 = m^2 k^2 > n^2$, soit $mk > n$, ce qui est impossible, donc soit $m^2 \leq n$, soit $k^2 \leq n$ (c'est-à-dire soit $m \leq \sqrt{n}$, soit $k \leq \sqrt{n}$). Dans le premier cas, on a $p^2 \leq m^2 \leq n$, dans le second on a $q^2 \leq k \leq n$, dans les deux cas $n$ possède un facteur premier $p$ tel que $p^2 \leq n$, et l'implication inverse est démontrée par contraposition. □

**Remarque 1.5.13.** Nous préférons énoncer la proposition et la démontrer à partir des carrés d'entiers plutôt que des racines carrées. Nous avons introduit l'ensemble $\mathbb{R}$ des nombres réels et la fonction racine carrée $\sqrt{\ }$ dans le cours n° 1 de ce semestre, mais nous prenons ici le parti de redéfinir tous les ensembles naturels et leurs propriétés à partir de $\mathbb{N}$. On peut bien sûr utiliser la racine carrée dans les applications si cela s'avère nécessaire, mais il est profitable d'apprendre à utiliser des encadrements par des entiers, comme dans l'exemple suivant et les exercices.

**Exemple 1.5.14.** L'entier 43 est-il premier ? On remarque que $6^2 = 36 < 43 < 7^2 = 49$ (donc $\sqrt{43} < 7$), donc par la proposition il suffit de tester les nombres premiers dont le carré est inférieur à 43, soit $2, 3$ et $5$. Comme 43 est impair et son chiffre des unités est différent de 5, et comme la somme de ses chiffres n'est pas divisible par 3 (voir la section 2.7.6), aucun de ces nombres n'est facteur premier de 43, qui est donc premier.

### Exercices de la section

*Exercice* 1.5.15. i) Calculer $2^7$, $35^3$ et $3^9$.
ii) Démontrer que 5 et 7 sont premiers en utilisant des divisions euclidiennes et le corollaire 1.4.9.
iii) Donner une autre démonstration du lemme 1.5.6 selon le schéma suivant. Si $n \geq 2$, on considère l'ensemble $D$ des diviseurs de $n$ qui sont $> 1$ : il possède un plus petit élément $m$. En raisonnant par l'absurde et en utilisant le lemme 1.5.5, montrer alors que $m$ est premier.
iv) Déterminer tous les nombres premiers inférieurs à 100.
v) Calculer $360^2$.

## 1.6 Plus grand commun diviseur

Soit $n$ un entier naturel : on a $n = 1 \times n$, donc on a toujours $1|n$, et si $n$ est non nul et $d$ est un diviseur de $n$, on a $d \leq n$ par l'exercice 1.3.17(v), si bien que l'ensemble $D(n)$ des diviseurs de $n$ est inclus dans l'ensemble $[[1, n]]$ et contient 1. Si $m$ est un autre entier naturel non nul, de même l'ensemble $D(m)$ des diviseurs de $m$ est inclus dans $[[1, m]]$ et contient 1, si bien que $1 \in D(n) \cap D(m) \subseteq [[1, n]] \cap [[1, m]]$. L'ensemble $D(n) \cap D(m)$ est l'ensemble des diviseurs communs à $n$ et à $m$; tous ses éléments sont alors inférieurs au plus petit des nombres $n$ et $m$, c'est-à-dire à $\min\{n, m\}$. Un sous-ensemble fini non vide de $\mathbb{N}$ possédant toujours un plus grand élément par le lemme 1.4.1, on peut poser la

**Définition 1.6.1.** Si $m$ et $n$ sont deux entiers naturels non tous deux nuls, le *plus grand commun diviseur de $m$ et $n$, noté $pgcd(m, n)$ ou $m \wedge n$*, est le plus grand entier naturel divisant à la fois $m$ et $n$.

Autrement dit, avec les notations du paragraphe précédent le p.g.c.d. de $m$ et $n$ est le plus grand élément de l'ensemble $D(m) \cap D(n)$ des diviseurs communs à $m$ et à $n$. Attention : si $m = n = 0$, on a $D(m) = D(n) = \mathbb{N}$, donc on ne peut définir le pgcd dans ce cas, d'où la précaution dans la définition. A la limite, si l'un seulement des deux nombres $m$ et $n$ est non nul, on peut encore définir le p.g.c.d de $m$ et $n$.

**Définition 1.6.2.** Deux entiers naturels $m$ et $n$ sont dits *premiers entre eux* si leur p.g.c.d. est 1.

**Exemple 1.6.3.** i) Les entiers naturels diviseurs de 12 sont $1, 2, 3, 4, 6$ et 12, et ceux de 15 sont $1, 3, 5, 15$. Ainsi, 1 et 3 sont les diviseurs communs de 12 et 15, qui ne sont donc pas premiers entre eux, puisque leur p.g.c.d est 3.

ii) Les entiers naturels diviseurs de 14 sont $1, 2, 7$ et 14, donc 14 et 15 sont prmeiers entre eux.

Dans l'Antiquité grecque, on définissait le processus appelé *antypharèse* ou *antyphérèse* comme la recherche de la plus grande unité de mesure commune à deux longueurs données $a$ et $b$, autrement dit de la plus grande longueur dont deux longueurs données sont des multiples entiers (voir la section 3.5). Le p.g.cCd de deux nombres entiers naturels est un analogue (en fait un cas particulier) de cette "mesure commune" entre deux longueurs.
Pour trouver cette mesure, on ordonne les deux grandeurs $a$ et $b$ et on soustrait la plus petite à la plus grande le nombre de fois nécessaire pour obtenir un "reste" strictement inférieur à $a$. Par exemple, si $a < b$ il existe un entier naturel $n$ tel que $na \leq b < (n+1)a$ et le nombre restant, $b - na$, est alors strictement inférieur à $a$, et on répète le procédé. Deux situations sont possibles :
i) soit le procédé "s'arrête" après un nombre fini d'étapes, et alors à la dernière étape où l'on trouve un reste non nul, ce reste est la mesure commune aux deux longueurs de départ
ii) soit le procédé "ne s'arrête jamais", et alors les deux longueurs sont "incommensurables" (elles ne peuvent être mesurées dans une unité commune).

Nous verrons dans le troisième chapitre de ce cours, à propos des nombres rationnels, que deux grandeurs rationnelles sont toujours commensurables, c'est-à-dire que l'algorithme précédent s'arrête toujours après un nombre fini d'étapes. Dans le cas qui nous intéresse ici, il est possible de s'inspirer de cet algorithme de détermination de la plus grande mesure commune, pour déterminer le plus grand commun diviseur de deux entiers naturels non nuls $m$ et $n$. Le procédé s'appelle **l'algorithme d'Euclide** et repose sur l'itération de la division euclidienne; nous le décrivons ici.
Rappelons et précisions une définition introduite dans la section 1.1 :

**Définition 1.6.4.** Une *suite* d'éléments d'un ensemble non vide $E$ est une application $u : \mathbb{N} \to E$. La valeur de $u$ en $n \in \mathbb{N}$, autrement dit l'élément $u(n)$ de $E$, est appelé le *terme d'indice* $n$ de la suite $u$, et est notée $u_n$.

**Remarque 1.6.5.** On désigne souvent une suite par l'ensemble de ses termes, plutôt que comme application. Ainsi, pour la suite de la définition, on écrira plutôt $(u_n)$ que $u$ : l'écriture sous-entend qu'on considère tous les éléments $u_n$. Une variante de cette écriture est $(u_n : n \in \mathbb{N})$; bien sûr, n'importe quel symbole peut servir à indexer les éléments d'une suite.

Soient $m$ et $n$ deux entiers naturels, tels que $m \geq n > 0$. Nous définissons une suite $(r_i : i \in \mathbb{N})$ d'entiers naturels comme suit, par récurrence sur $i$. Si $i = 0$, on pose $r_0 = n$ et la division euclidienne de $m$ par $n$ permet d'écrire $m = nq_1 + r_1 = r_0q_1 + r_1$ avec $r_1 = 0$ ou bien $0 < r_1 < r_0 = n$. De même, si $r_1 > 0$, la division euclidienne de $n = r_0$ par $r_1$ s'écrit $r_0 = r_1q_2 + r_2$ avec $r_2 = 0$ ou $0 < r_2 < r_1$. En général, supposons que $r_0, \ldots, r_n$ sont définis pour $n \geq 1$ :
- si $r_n = 0$, on pose $r_{n+1} = 0$
- si $r_n > 0$, on peut effectuer la division euclidienne de $r_{n-1}$ par $r_n$ sous la forme

$r_{n-1} = r_n q + r$ avec $r = 0$ ou $0 < r < r_n$, et on pose alors $r_{n+1} = r$.
Par unicité du quotient et du reste de la division euclidienne, à chaque étape $r_n$ est bien défini, et par récurrence on obtient une suite $(r_n)$ d'entiers naturels.

**Exemple 1.6.6.** Illustrons l'algorithme avec $m = 543$ et $n = 127$. On a $r_0 = 127$, et la division de 543 par 127 nous donne le reste $r_1 = 15$. La division de $r_0$ par $r_1$ donne le reste $r_2 = 7$, puis la division de $r_1$ par $r_2$ donne le reste $r_3 = 1$, et enfin la division de $r_2$ par $r_3$ donne le reste $r_4 = 0$. La suite $(r_n)$ est donc donnée par : $r_0 = 127$, $r_1 = 15$, $r_2 = 7$, $r_3 = 1$, et $r_n = 0$ pour tout $n \geq 4$.

**Lemme 1.6.7.** *Pour tout entier naturel $i$, si $r_i > 0$ on a $0 < r_i < r_{i-1} < \ldots < r_0$. En particulier, il existe $i \in \mathbb{N}$ tel que $r_i = 0$.*

*Démonstration.* Nous procédons par récurrence sur $i$. Si $i = 0$, le premier énoncé est vrai (il se réduit à "$0 < r_0$") puisque $r_0 = n > 0$ par hypothèse. Si $i = 1$, on a $m = nq_1 + r_1$ avec $0 < r_1 < n = r_0$ par définition du reste de la division euclidienne. Supposons que $i \geq 2$ : $i$ est alors de la forme $j + 2$, et par définition en divisant $r_j$ par $r_{j+1}$ on a $r_j = r_{j+1}q + r_i$, avec $r_i = r_{j+2} < r_{j+1}$ à nouveau. Il s'ensuit que $r_i < r_{j+1} = r_{i-1} < r_j < \ldots < r_0$ par hypothèse de récurrence, et l'énoncé est démontré au rang $i$. Par récurrence, le premier énoncé est démontré pour tout $i \in \mathbb{N}$. Supposons que pour tout $i \in \mathbb{N}$, nous ayons $r_i \neq 0$ : par ce qui précède, l'ensemble $E = \{r_i : i \in \mathbb{N}\}$, image de la suite $(r_i)$, ne possède pas de plus petit élément; en effet, si $r_i \in E$, comme $r_{i+1} > 0$ on a $r_{i+1} \in E$ et $r_{i+1} < r_i$, donc $r_i$ ne peut être le plus petit élément de $E$ pour aucun indice $i$. Comme l'ensemble $E$ n'est pas vide, ceci contredit le fait que tout sous-ensemble non vide de $\mathbb{N}$ possède un plus petit élément (proposition 1.4.3). Par *reductio ad absurdum*, nous concluons qu'il existe $i \in \mathbb{N}$ tel que $r_i = 0$. □

**Lemme 1.6.8.** *Si $m \geq n > 0$ comme avant et $m = nq + r$ est la division euclidienne de $m$ par $n$, alors $pgcd(m, n) = pgcd(n, r)$.*

*Démonstration.* Soit $d \in \mathbb{N}$, $d \geq 2$, tel que $d$ divise $m$ et $n$ : par le lemme 1.5.8, on a $d|m - nq = r$, donc $d$ divise $n$ et $r$. Inversement, si $d$ divise $n$ et $r$, alors $d|m = nq + r$ (puisqu'il existe $u, v \in \mathbb{N}$ tels que $n = du$ et $r = dv$, d'où $m = nq + r = duq + dv = d(uq + v)$), donc $d$ divise $m$ et $n$. Les couples $(m, n)$ et $(n, r)$ ont donc les mêmes diviseurs positifs, ils ont donc le même pgcd. □

L'algorithme d'Euclide est le procédé qui est justifié par la proposition suivante, laquelle en établit le principe de manière rigoureuse grâce à un lemme simple.

**Lemme 1.6.9.** *L'ensemble des indices $i \in \mathbb{N}$ pour lesquels $r_i > 0$ est fini.*

*Démonstration.* Par le lemme 1.6.7, il existe $i_0 \in \mathbb{N}$ tel que $r_{i_0} = 0$. Montrons que pour tout $i \geq i_0$, on a $r_i = 0$ : si $i \geq i_0$, il existe $j \in \mathbb{N}$ tel que $i = i_0 + j$, et on procède par récurrence sur $j$. Si $j = 0$, on a $i = i_0$ et $r_i = r_{i_0} = 0$; supposons que la propriété est vérifiée au rang $j \geq 0$, c'est-à-dire que $r_{i_0+j} = 0$ : par définition de $r_{(i_0+j)+1}$, on a alors $r_{i_0+(j+1)} = 0$, ce qui est la propriété au rang $j + 1$. Par le principe de récurrence, on a $r_{i_0+j} = 0$ pour tout $j \in \mathbb{N}$, soit $r_i = 0$ pour tout $i \geq i_0$. Il s'ensuit que l'ensemble $\{i \in \mathbb{N} : r_i > 0\}$ est inclus dans l'ensemble $[[0, i_0]]$, il est donc fini. □

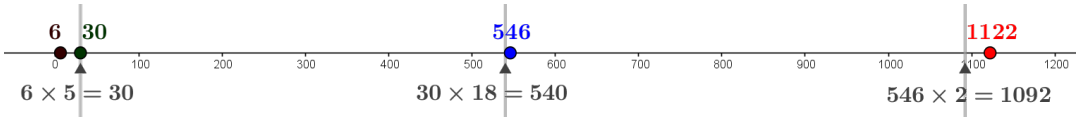



Figure 6: Illustration de l'algorithme d'Euclide appliqué à 1122 et 546 : les deux nombres doivent être "mesurés" l'un par rapport l'autre jusqu'à ce que l'on obtienne la "plus petite commune mesure", qui est leur p.g.c.d., à savoir 6.

**Proposition 1.6.10** (Algorithme d'Euclide)**.** *Pour tous entiers naturels $m \geq n > 0$ et pour tout entier naturel $i$ tel que $r_i > 0$, on a $pgcd(m,n) = pgcd(r_i, r_{i+1})$. En particulier, le dernier reste non nul dans la suite $(r_i : i \in \mathbb{N})$ est le p.g.c.d. de $m$ et de $n$.*

*Démonstration.* Nous procédons à nouveau par récurrence sur $i$. Si $i = 0$, on a $r_0 = n$ et $r_1$ est le reste de la division euclidienne de $m$ par $r_0 = n$, si bien que par le lemme 1.6.8, on a $pgcd(m,n) = pgcd(r_0, r_1)$. Supposons que $r_{i+1} > 0$ et que le résultat soit vrai au rang $i$, c'est-à-dire que $pgcd(m,n) = pgcd(r_i, r_{i+1})$ (puisque $r_i > 0$) : par définition, $r_{i+2}$ est le reste de la division de $r_i$ par $r_{i+1}$, de sorte que par le lemme 1.6.8 à nouveau, on a $pgcd(r_i, r_{i+1}) = pgcd(r_{i+1}, r_{i+2})$, soit $pgcd(m,n) = pgcd(r_{i+1}, r_{i+2})$, ce qui est la propriété au rang $i+1$, et la propriété est donc valide pour tout $i \in \mathbb{N}$ par récurrence. En ce qui concerne la dernière assertion, dire que $r_j$ est le dernier reste non nul dans la suite $(r_i : i \in \mathbb{N})$, c'est dire que $j$ est le plus grand entier naturel $i$ tel que $r_i \neq 0$. Par lemme 1.6.9, l'ensemble $\{i \in \mathbb{N} : r_i > 0\}$ est fini et par le lemme 1.4.1 il possède donc un plus grand élément $j$. Par ce qui précède, on a $pgcd(m,n) = pgcd(r_j, r_{j+1}) = pgcd(r_j, 0) = r_j$, puisque $r_j | 0$. □

**Remarque 1.6.11.** i) On rencontre parfois cet énoncé sous la forme : "pour tout $i \in \mathbb{N}$, on a $pgcd(m,n) = pgcd(r_i, r_{i+1})$". Cette forme est inexacte, puisque le p.g.c.d. de 0 et 0 n'est pas défini : si $r_i = 0$, alors $r_{i+1} = 0$ aussi par définition.
ii) Il paraît évident que la suite des $r_i$ est "nulle à partir d'un certain rang", mais il faut l'établir rigoureusement pour pouvoir désigner le "dernier reste non nul" dans l'algorithme d'Euclide.

Dans la pratique, on peut effectuer les divisions successives en alternant le choix du diviseur et du dividende. Par exemple, pour trouver le p.g.c.d. de 546 et de 1122, sans décomposition en nombres premiers, on écrit les divisions successives suivantes :
- $1122 = 546 \times 2 + 30$ : $r_0 = 546$, $r_1 = 30$
- $546 = 30 \times 18 + 6$ : $r_1 = 30$, $r_2 = 6$
- $30 = 6 \times 5 + 0$ : $r_2 = 6$, $r_3 = 0$.

Par la proposition 1.6.10, puisque $r_2 = 6$ et $r_3 = 0$, le p.g.c.d. de 546 et 1122 est 6. On aurait pu le trouver également avec une décomposition en nombres premiers des deux nombres sous la forme $546 = 2 \times 3 \times 7 \times 13$ et $1122 = 2 \times 3 \times 11 \times 17$. L'utilisation de la décomposition en nombres premiers est avantageuse pour des petits nombres facilement décomposables, mais dès que les nombres atteignent une certaine taille, l'algorithme d'Euclide est plus puissant.
La figure 6 présente une application de l'algorithme d'Euclide.

### Exercices de la section

*Exercice* 1.6.12. i) En décomposant les nombres 21 et 55 en produit de nombres premiers, établir la liste de leurs diviseurs et démontrer qu'ils sont premiers entre eux.
ii) En utilisant une décomposition en facteurs premiers, déterminer le p.g.c.d. des nombres 84 et 90.
ii) En utilisant l'algorithme d'Euclide, déterminer le p.g.c.d. de 1130 et 2145.
iii) Quels sont tous les nombres premiers à 231 qui lui sont inférieurs ? Indication : déterminer tous les nombres qui ne sont pas premiers à 231.

## 1.7 Décomposition dans une base numérique

Lorsque nous écrivons un entier naturel $n$ donné sous une forme explicite, nous utilisons habituellement le système décimal, ce qui signifie que nous "représentons" ce nombre dans la *base numérique* 10.
Nous considérons la plus grande puissance de 10, notons-là $10^m$, qui est inférieure à $n$, puis nous effectuons la division euclidienne de $n$ par $10^m$, soit $n = 10^m.q + r$, avec $0 \leq r < 10^n$. Le quotient $q$ est le premier chiffre de l'écriture décimale de $n$, et nous prenons le reste $r$ pour recommencer l'opération avec la plus grande puissance de 10 inférieure à $r$, et ainsi de suite jusqu'à obtenir un reste $< 10$.
Les quotients successifs sont alors écrits dans une suite, qu'on termine par le dernier reste, et qui est l'écriture usuelle de $n$ en base 10 (dans laquelle on a éventuellement placé des zéros, correspondant aux puissances de 10 qui n'apparaissent pas dans le processus).

**Exemple 1.7.1.** Soit $n = 3207$. La plus grande puissance de 10 inférieure à $n$ est $1000 = 10^3$, et on a $3207 = 3.1000 + 207$ avec $207 < 1000$, donc 3 est le quotient et 207 est le reste de la division euclidienne de 3207 par 1000 : nous enregistrons 3 comme le premier chiffre du développement. Alors, $100 = 10^2$ est la plus grande puissance de 10 qui est $\leq 207$, et $207 = 2.100 + 7$ est la division euclidienne de 207 par 100, de quotient 2 et de reste 7, et nous retenons 2. Comme 10 n'est pas $\leq 7$, à cette étape on doit retenir 0 (on a $7 = 0.10 + 7$), et comme $7 < 10$, le processus est terminé et nous enregistrons 7 comme le dernier chiffre du développement décimal, qui est donc donné par $3, 2, 0, 7$, écriture habituelle de $n$.

Sur le plan de la théorie mathématique, l'utilisation de 10 comme base de numération est une pure question de convention (sans aucun doute établie par la pratique de compter sur dix doigts !).
Mathématiquement, cette "décomposition" implicite d'un entier naturel apparaît dans son écriture courante mais peut s'appliquer à toute autre base de numération. Par exemple, en base 2 on obtient l'écriture dite *binaire*, ubiquitaire en informatique théorique et dans les systèmes informatiques. Nous voulons ici décrire ce principe en détail, qui sera développé ultérieurement jusque dans la théorie des nombres réels.
Etant donné un entier naturel $b > 1$ pris comme base de numération, la première chose à faire est d'établir l'existence d'une "plus grande puissance de $b$" inférieure à un entier naturel non nul donné.

**Lemme 1.7.2.** *Soient $b, m \in \mathbb{N}$ tels que $m > 0$ et $b > 1$. Il existe alors un unique entier $k \in \mathbb{N}$ tel que $b^k \leq m < b^{k+1}$.*

*Démonstration.* On procède par récurrence sur $m$ pour démontrer d'abord l'existence de $k$. Si $m = 1$, on a $b^0 = 1 \leq m < b^1 = b$, donc la propriété est vraie au rang $m = 1$. Supposons, par récurrence, qu'il existe un unique entier $k$ tel que $b^k \leq m < b^{k+1}$ : on distingue alors deux cas. Si $m + 1 < b^{k+1}$, on a $b^k \leq m < m + 1 < b^{k+1}$, donc l'entier $k$ convient. Sinon, on a $m + 1 = b^{k+1}$ (car $m < b^{k+1}$), et comme $b^{k+1} < b^{k+2} = b^{k+1}.b$ (ce qui se montre par récurrence sur $k$ !), l'entier $k + 1$ convient, puisqu'alors $b^{k+1} = m + 1 < b^{k+2}$, et on conclut par le principe de récurrence. En ce qui concerne l'unicité, supposons que $b^{k'} \leq m < b^{k'+1}$, mais que $k \neq k'$ : par exemple, si $k < k'$, on a alors $k + 1 \leq k'$, si bien que $m < b^{k+1} \leq b^{k'} \leq m$, d'où $m < m$, ce qui est impossible, et par *reductio ad absurdum*, on a donc $k = k'$ (le cas $k > k'$ se traite de la même façon), d'où l'unicité de $k$. □

L'étape suivante consiste à considérer la décomposition d'un nombre entier naturel $m$ dans une base numérique $b > 1$, c'est-à-dire sous la forme d'une suite de "chiffres" qui sont des entiers naturels compris entre 0 et $b - 1$, et dont les positions dénotent les puissances successives de $b$. On s'appuie sur l'idée que si $b^k$ est la plus grande puissance apparaissant dans le développement de $m$, alors on doit avoir $m < b^{k+1}$.

**Lemme 1.7.3.** *Soient $k$ un entier naturel et $(m_0, \ldots, m_k)$ une suite finie de $k + 1$ entiers strictement inférieurs à un entier $b > 1$. Si $m = \sum_{i<k+1} m_i.b^i$, alors on a $m < b^{k+1}$.*

*Démonstration.* Pour tout $i \leq k$, on a $m_i < b$ par hypothèse, c'est-à-dire $m_i \leq b-1$. On a donc $m = 1.m^1 \leq \sum_{i=0}^{k+1}(b-1).m^i = (b-1).\sum_{i=0}^{k+1} b^i = (b-1).\dfrac{b^{k+1}-1}{b-1} = b^{k+1} - 1$; autrement dit, on a $m < b^{k+1}$. On peut aussi le démontrer sans la formule de la somme, par récurrence sur $k$. Si $k = 0$, on a par hypothèse $m = m_0 < b = b^1 = b^{k+1}$ donc la propriété est vérifiée. Si la propriété est vérifiée au rang $k$ et $(m_0, \ldots, m_{k+1})$ est une suite finie de $k + 2$ entiers strictement inférieurs à $b$, on a $m = \sum_{i=0}^{k+1} m_i.b^i = \sum_{i=0}^{k+1} m_i.b^i + m_{k+1}.b^{k+1} < b^{k+1} + m_{k+1}.b^{k+1}$ (par hypothèse de récurrence) $\leq b^{k+1} + (b-1).b^{k+1}$ (parce que $m_{k+1} \leq b-1$) $= (1+b-1).b^{k+1} = b^{k+2}$, donc la propriété est vraie au rang $k + 1$. Par le principe de récurrence, elle est démontrée. □

**Remarque 1.7.4.** i) La formule de la somme des $k + 1$ nombres $1, b, \ldots, b^k$ lorsque $b \neq 1$ est établie par récurrence dans le dernier chapitre du cours n°1. L'étudiant(e) peut la redémontrer directement au besoin.

**Exemple 1.7.5.** Pour $b = 10$, une suite de $n$ chiffres $a_0, \ldots, a_{n-1} \in \{0, \ldots, 9\}$ détermine le nombre $m = a_0 + a_1.10 + a_2.10^2 + \ldots + a_{n-1}.10^{n-1}$, qui est toujours strictement inférieur à $10^n$ et qu'on écrit $a_{n-1}a_{n-2}\ldots a_2a_1a_0$ dans le système décimal usuel. Par exemple, pour $n = 3$, $a_0 = 9$, $a_1 = 0$ et $a_2 = 4$, on obtient $m = 9 + 0.10 + 4.10^2 = 409$, qui est bien strictement inférieur à $10^3 = 1000$.

A partir de ces résultats préliminaires, il est possible d'établir rigoureusement la décomposition d'un entier naturel dans une base numérique quelconque, sous la forme suivante.

**Théorème 1.7.6** (Bases de numération)**.** *Soient $b$ et $m$ deux entiers naturels, avec $b > 1$. Il existe un entier naturel $k$ et suite finie de $k+1$ entiers naturels $(m_0, \dots, m_k)$ tous strictement inférieurs à $b$, et tels que $m = \sum_{i=0}^{k} m_i.b^i$. De plus, si $m \neq 0$, il existe un unique entier $k$ et une unique suite $(m_0, \dots, m_k)$ avec cette propriété et tels que $m_k \neq 0$.*

*Démonstration.* Si $m = 0$, alors $m = 0 = 0.b^0$, donc l'existence de la suite est démontrée dans ce cas, avec $k = 0$ et $m_0 = 0$. Si $m \neq 0$, par le lemme 1.7.2, il existe un unique entier naturel $k$ tel que $b^k \leq m < b^{k+1}$ : on démontre d'abord l'existence de la suite $(m_0, \dots, m_k)$ par récurrence sur $k$. Si $k = 0$, on a $m < b$ et donc $m = m_0.l^0$ pour $m_0 = m$ : la suite $(m_0)$ convient. Si la propriété est vraie au rang $k$, supposons que $b^{k+1} \leq m < b^{k+2}$. En effectuant la division euclidienne de $m$ par $b^{k+1}$, on obtient deux nombres entiers uniques $q$ et $r$ tels que $m = q.b^{k+1} + r$, avec $r < b^{k+1}$. Soit $E$ l'ensemble des entiers naturels $n$ tels que $r < b^{n+1}$ : $E$ n'est pas vide (il contient $k$), donc par la proposition 1.4.3 il en existe un plus petit élément, notons le $k'$ : on a $k' \leq k$, et $b^{k'} \leq r < b^{k'+1}$. Par l'hypothèse de récurrence appliquée à $k'$, il existe une suite $(r_0, \dots, r_{k'})$ de $k'+1$ entiers strictement inférieurs à $b$, et tels que $r = \sum_{i=0}^{k'} r_i.b^i$ : on pose $m_i = r_i$ pour tout $i < k'+1$, $m_i = 0$ pour tout $i$ tel que $k'+1 \leq i < k+1$ s'il y a lieu, et $m_{k+1} = q$. On a alors $m = q.b^{k+1} + r = \sum_{i=0}^{k+1} m_i.b^i$, ce qui est la propriété au rang $k+1$. Par récurrence, on en déduit l'existence de la suite $(m_0, \dots, m_k)$.
En ce qui concerne l'unicité, supposons que $m \neq 0$. D'abord, par ce qui précède on peut écrire $m = \sum_{i=0}^{k} m_i.b^i$. Comme $m \neq 0$, il existe $i \in \{0, \dots, k\}$ tel que $m_i \neq 0$ (sinon, on a $m = \sum_{i=0}^{k} 0.b^i = 0$) et on peut supposer que $m_k \neq 0$, quitte à supprimer des termes nuls dans la somme (écrire $m = \sum_{i=0}^{k'} m_i.b^i$, où $k'$ est le plus grand entier $i$ tel que $m_i \neq 0$, et renommer $k'$ en $k$). Montrons l'unicité de de $k$ et de la suite $(m_i : i < k+1)$ avec ces propriétés. Soient donc $k'$ un entier et $(m_i : i < k'+1)$ une suite d'entiers strictement inférieurs à $b$ et tels que $m = \sum_{i<k'+1} m'_i.b^i$ avec $m'_{k'} \neq 0$; par le lemme 1.7.3 on a $m < b^{k+1}$ et $m < b^{k'+1}$, et on a aussi $b^k \leq m_k.b^k \leq m$ puisque $m_k \neq 0$, et de même $b^{k'} \leq m$. Par le lemme 1.7.2, on en déduit que $k = k'$, et on va montrer par récurrence sur $k$ que $m_i = m'_i$ pour tout $i < k+1$. Si $k = 0$, on a $m = m_0 = m'_0$ et la propriété est vérifiée. Si la propriété est vérifiée au rang $k''$ et $k = k''+1$, on écrit $m = r + m_k.b^k = r' + m'_k.b^k$ avec $r = \sum_{i<k''+1} m_i.b^i < b^{k''+1} = b^k$ et $r' = \sum_{i<k''+1} m'_i.b^i < b^k$. Par le lemme 1.7.3 à nouveau, on a $r, r' < b^{k''+1}$, soit $r, r' < b^k$, donc par unicité du quotient et du reste de la division euclidienne de $m$ par $b^k$, $m_k = m'_k$ est le quotient de cette division, et $r = r'$ est le reste de cette division. Par hypothèse de récurrence appliquée à $r$, on a également $m_i = m'_i$ pour tout $i < k$, et la preuve est achevée par récurrence. □

**Exemple 1.7.7.** Choisissons $b = 3$. Le nombre écrit sous la forme "1210" en base 3 est le nombre $0 \times 3^0 + 1 \times 3^1 + 2 \times 3^2 + 1 \times 3^3 = 3 + 18 + 27 = 48$ (écrit en base 10...). Pour retrouver l'écriture de 48 en base 3, on utilise la décomposition selon le schéma présenté ici : on a $3^3 = 27 \leq 48 < 3^4 = 81$, donc $3^3$ est la plus grande puissance de 3 qui est inférieure à 48. Les divisions euclidiennes successives donnent : $48 = 27 \times 1 + 21$, $21 = 9 \times 2 + 3$ et $3 = 3 \times 1 + 0$, donc en prenant les quotients successifs et le dernier reste on obtient l'écriture $1, 2, 1, 0$ en base 3.

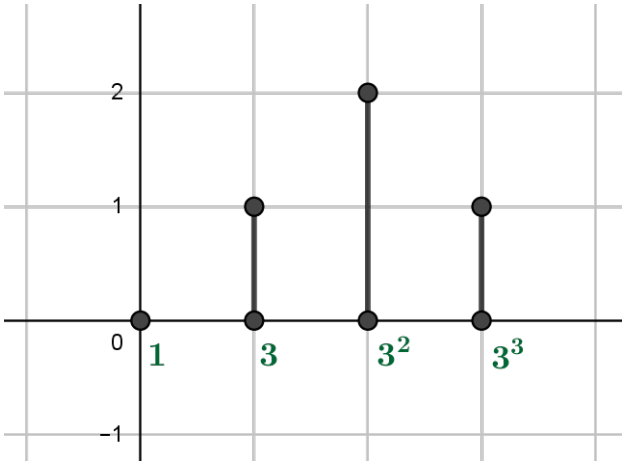



Figure 7: Décomposition du nombre $48 = 0 \times 1 + 1 \times 3 + 2 \times 3^2 + 1 \times 3^3$ en base 3 : le chiffre des unités est 0, celui des "3-aines" est 1, celui des "9-aines" est 2 et celui des "27-aines" est 1. L'échelle des abscisses est "géométrique" : on passe d'une graduation à l'autre par une multiplication par 3.

La figure 7 propose une représentation graphique de la décomposition de l'entier 48 en base 3.

## Exercices de la section

*Exercice* 1.7.8. i) Quel est le nombre dont l'écriture en base 7 est $2, 0, 1, 3$ ?
ii) On complète la série des chiffres usuels $0, 1, 2, \ldots, 9$ par les lettres $A, B, C, D, E, F$ dans cet ordre, pour écrire les nombres en base 16 (système "hexadécimal"). Ecrire les nombres $10, 11, 12, 13, 14, 15$ et 16 en base 16. Quel est le nombre dont l'écriture en base 16 est $1C$ ? le nombre dont l'écriture en base 16 est 100 ?
iii) En effectuant la division euclidienne de 237 par la plus grande puissance de 16 qui le divise, écrire 237 en base 16 grâce à la numération hexadécimale.
iv) Ecrire les nombres suivants en base 2 : 1, 2, 4, 8, 16, 24, 48, 96.
v) Ecrire le nombre 195 en base 3.

# Chapitre 2

# L'ensemble $\mathbb{Z}$ des nombres entiers relatifs

Dans le premier chapitre, nous avons énoncé rigoureusement les trois axiomes de Peano, concernant la fonction successeur $s : \mathbb{N} \to \mathbb{N}$, $n \mapsto n+1$, et nous en avons déduit de nombreuses propriétés de l'ensemble $\mathbb{N}$, ainsi qu'une définition des opérations usuelles $+$ et $\times$, et des relations d'ordre naturel $\leq$ et $<$.
Ainsi, toute l'arithmétique naturelle, c'est-à-dire la théorie opératoire et relationnelle des nombres entiers naturels, repose sur ces trois axiomes, qui déterminent entièrement l'ensemble $\mathbb{N}$. Ceci illustre la puissance et la fécondité de cette "méthode axiomatique", connue depuis l'Antiquité et de manière intuitive à travers la géométrie d'Euclide, mais appliquée ici à la racine de l'édifice mathématique de manière totalement transparente, grâce à la théorie naïve des ensembles.
Or, on peut prolonger la description de la "structure naturelle de l'ensemble $\mathbb{N}$" grâce à l'axiomatique de Peano, par la *construction*, parfaitement rigoureuse, des ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, et ceci sans axiomes supplémentaires. C'est ce que nous aborderons au second semestre, à partir d'un approfondissement de la théorie des ensembles.
Dans ce chapitre, nous allons plutôt adopter une approche *axiomatique* pour la description de l'ensemble $\mathbb{Z}$, auquel nous prolongerons les opérations et relations naturelles de l'ensemble $\mathbb{N}$. Nous pourrons alors exposer la théorie arithmétique élémentaire des nombres entiers *relatifs*, passablement plus élaborée que l'arithmétique des entiers naturels, qu'elle approfondit de manière lumineuse grâce à la soustraction. Et ceci, bien qu'elle soit contenue en germe dans les trois petits axiomes de Peano qui ouvrent ce livre.

## 2.1 Description axiomatique de l'ensemble $\mathbb{Z}$

Comme nous l'avons fait pour l'ensemble $\mathbb{N}$ dans la section 1.1 et dans les cours n° 1 et 2, nous admettons ici l'existence d'un ensemble $\mathbb{Z}$ des nombres entiers relatifs, que nous concevons de manière intuitive comme dans le cours n° 1, et qui contient l'ensemble $\mathbb{N}$ comme sous-ensemble.
A ce niveau du cursus, nous ne démontrons pas "l'existence" de cet ensemble, mais nous en donnons une description par des axiomes, comme nous l'avons fait pour

l'ensemble $\mathbb{N}$.

## Axiomatisation de $\mathbb{Z}$ à partir de l'addition

Dans le cours n° 1, nous avons énoncé quelques propriétés élémentaires de l'ensemble $\mathbb{Z}$. La formulation d'un système d'axiomes consiste à exprimer de telles propriétés mais en les choisissant judicieusement, de manière à décrire l'essentiel de la "structure arithmétique" de cet ensemble, qui nous intéresse dans ce volume.
Ici l'approche la plus naturelle nous paraît consister dans l'axiomatisation de *l'addition* (et de la soustraction) des entiers relatifs, c'est-à-dire que nous admettons l'existence d'une application $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, prolongeant l'addition des entiers naturels, et possédant les propriétés axiomatiques suivantes :

**Axiome 2.1.1.** *i) Pour tout $n \in \mathbb{Z}$ on a $0 + n = n$*
*ii) Pour tous $n, m \in \mathbb{Z}$, on a $n + m = m + n$ (l'addition est commutative)*
*iii) Pour tous $n, m, k \in \mathbb{Z}$, on a $(n+m)+k = n+(m+k)$ (l'addition est associative)*
*iv) Pour tout $n \in \mathbb{Z}$, il existe $m \in \mathbb{Z}$ tel que $n + m = 0$ (tout élément possède un opposé pour l'addition).*

**Remarque 2.1.2.** Dire que l'addition des entiers relatifs *prolonge* celle des entiers naturels, cela signifie que pour $n, m \in \mathbb{N}$, le résultat de l'opération $n + m$ dans $\mathbb{Z}$ (puisque $\mathbb{N} \subseteq \mathbb{Z}$) est la somme $n + m$ telle qu'elle a été définie à la section 1.2, ou encore, que l'addition $+_{\mathbb{N}} : \mathbb{N}^2 \to \mathbb{N}$ des entiers naturels est la restriction de $+$ à $\mathbb{N}$, soit $+_{\mathbb{N}} = +|_{\mathbb{N}}$.

Par la propriété (iv) de l'axiome 2.1.1, tout nombre entier relatif possède un *opposé* pour l'addition : c'est la propriété fondamentale que ne possède pas l'ensemble $\mathbb{N}$ et qui fait l'intérêt arithmétique de l'ensemble $\mathbb{Z}$.
L'opposé additif $m$ d'un entier relatif $n$ est nécessairement unique : en effet, si $k \in \mathbb{Z}$ et $n + k = 0$, alors on a $m = 0 + m$ (par (i)) $= m + 0$ (par (ii)) $= m + (n + k) = (m + n) + k$ (par (iii)) $= (n + m) + k$ (par (ii)) $= 0 + k = k + 0$ (par (ii)) $= k$ (par (i)). On note $-n$ l'opposé additif de $n$, et on *définit* la **différence** $n - m$ de deux entiers relatifs $n$ et $m$ comme l'entier relatif $n + (-m)$.

**Définition 2.1.3.** L'application $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, qui associe à un couple d'entiers relatifs $(n, m)$ la différence $n-m = n+(-m)$, est la *soustraction* des entiers relatifs.

Les propriétés de l'axiome 2.1.1 ne suffisent pas à caractériser l'ensemble $\mathbb{Z}$, c'est-à-dire à le décrire de manière essentiellement unique. Pour compléter cette description axiomatique, il nous faut introduire un axiome fondamental qui permet de situer les entiers relatifs par rapport aux entiers naturels :

**Axiome 2.1.4.** *Pour tout entier relatif $n$, soit $n$ est un entier naturel, soit $-n$ est un entier naturel.*

On peut alors démontrer, dans le même esprit que le problème 1.1.8, que l'ensemble $\mathbb{Z}$ ainsi décrit est "essentiellement unique".
La soustraction possède des propriétés analogues aux propriétés axiomatiques de l'addition et associées à celles-ci. Mentionnons trois d'entre elles, élémentaires mais essentielles :

**Proposition 2.1.5.** *Soient $m$ et $n$ deux entiers relatifs.*
*o) On a $-(-n) = n$*
*i) On a $-(m+n) = -m-n$*
*ii) On a $-(m-n) = n-m$.*

*Démonstration.* o) Par définition, $-(-n)$ est l'unique entier relatif $k$ tel que $(-n)+k = 0$, soit $0 = (-n)+(-(-n)) = 0$. En ajoutant $n$ aux deux membres, il vient $n = 0+n = (-(-n)+(-n))+n$ (par commutativité de l'addition) $= -(-n)+((-n)+n)$ (par associativité de l'addition) $= -(-n)+(n+(-n)) = (-n)+0 = -(-n)$, ce qu'il fallait démontrer.
i) Par définition, l'entier $-(m+n)$ est l'unique entier relatif $k$ tel que $(m+n)+k = 0$. Or on a $(m+n)+(-m-n) = (m+n)+(-n-m)$ (par commutativité de l'addition) $= m+(n+(-n-m))$ (par associativité de l'addition) $= m+((n+(-n))-m)$ (par associativité à nouveau) $= m+(0-m) = m-m = 0$, donc $-(m+n) = -m-n$.
ii) Par (i), on a $-(m-n) = -m-(-n) = -m+n$ (par (o)) $= n-m$. □

Notons enfin que tout nombre entier relatif $n$ peut toujours se représenter comme la différence de deux nombres entiers *naturels*. Par exemple, si $n \in \mathbb{N}$ on a $n = n-0$, et si $n \notin \mathbb{N}$ on a $-n \in \mathbb{N}$ par l'axiome 2.1.4, d'où $n = 0-(-n)$ par la proposition 2.1.5). Ces représentations "standard" ne sont toutefois pas uniques, et il existe pour tout entier relatif $n$ une infinité de représentations de $n$ comme différence de deux entiers naturels. En effet, si $n \in \mathbb{N}$, alors pour tout $k \in \mathbb{N}$ on a $n = (n+k)-k$, tandis que si $n \in \mathbb{Z}-\mathbb{N}$, alors pour tout $k \in \mathbb{N}$ on a $n = k-(k-n)$ (puisque $-n \in \mathbb{N}$). Et on a bien sûr $0 = k-k$ pour tout $k \in \mathbb{N}$.

**Exemple 2.1.6.** Le nombre entier 2 se représente par exemple comme $2 = 5-3$ ou encore $2 = 128-126$, et de manière générale pour tout entier naturel $k$, comme $2 = (2+k)-2$. De même, l'entier $-5$ se représente par exemple comme $-5 = 5-10$, ou encore $-5 = 247-252$, et de manière générale comme $-5 = k-(k+5)$ pour tout entier naturel $k$.

## L'ordre naturel dans $\mathbb{Z}$

Par définition, l'addition des entiers relatifs "prolonge" celle des entiers naturels, au sens où la seconde est la restriction de la première à l'ensemble $\mathbb{N}$. Une autre façon de le concevoir est de considérer que l'addition des entiers relatifs est un *prolongement* de celle des entiers naturels.
Or, la "structure naturelle" de l'ensemble $\mathbb{N}$, décrite au premier chapitre, fait aussi apparaître l'ordre naturel, défini à partir de l'addition dans la section 1.3.1, sous sa forme d'ordre large $\leq$ ou d'ordre strict $<$ (dit linéaire). Par analogie avec le prolongement de l'addition de l'ensemble $\mathbb{N}$ à l'ensemble $\mathbb{Z}$, on peut prolonger les relations d'ordre large et d'ordre strict à l'ensemble $\mathbb{Z}$.
Dans le chapitre 3 du cours n° 1, nous avons remarqué les analogies, les relations et les différences intuitives entre l'ordre naturel sur $\mathbb{N}$ et l'ordre naturel sur $\mathbb{Z}$. Nous utilisons ici ces remarques pour *définir* ce dernier :

**Définition 2.1.7.** Si $n$ et $m$ sont deux nombres entiers relatifs, on dit que :
i) *$n$ est inférieur (ou égal) à $m$*, ce qu'on note encore $n \leq m$, si il existe un entier

*naturel* $k$ tel que $n + k = m$
ii) $n$ *est strictement inférieur à* $m$, ce qu'on note encore $n < m$, si il existe un entier naturel *non nul* $k$ tel que $n + k = m$.

Par la définition 1.3.2 et la proposition 1.3.6, on s'aperçoit immédiatement que l'ordre naturel et l'ordre strict dans $\mathbb{Z}$ prolongent respectivement l'ordre naturel et l'ordre strict dans $\mathbb{N}$, dans le sens où si $m$ et $n$ sont deux entiers *naturels*, alors on a $m \leq n$ dans $\mathbb{Z}$ si et seulement si $m \leq n$ dans $\mathbb{N}$, et $m < n$ dans $\mathbb{Z}$ si et seulement si $m < n$ dans $\mathbb{N}$.
Pour être absolument rigoureux, nous aurions du introduire une notation différente pour ces relations dans $\mathbb{Z}$ et leurs contreparties dans $\mathbb{N}$, mais cette dernière remarque permet précisément d'adopter de manière un peu abusive la même notation pour les relations d'ordre large et strict dans les deux ensembles.
Les propriétés élémentaires de l'ordre large sur $\mathbb{Z}$ sont les suivantes :

**Proposition 2.1.8.** *Soient* $m, n, k$ *trois entiers relatifs.*
*o) On a* $m \leq m$ *(réflexivité)*
*i) Si* $m \leq n$ *et* $n \leq m$*, alors* $m = n$ *(antisymétrie)*
*ii) Si* $m \leq n$ *et* $n \leq k$*, alors* $m \leq k$ *(transitivité).*
*iii) On a* $n \geq 0 \Leftrightarrow n \in \mathbb{N}$.

*Démonstration.* o) On a $m + 0 = m$, et comme $0 \in \mathbb{N}$, par définition on a $m \leq m$.
i) Par définition, il existe $k, l \in \mathbb{N}$ tels que $m + k = n$ et $n + l = m$, d'où $m + (k + l) = (m + k) + l = n + l = m$, et en ajoutant $-m$ aux deux membres on obtient $0 = (-m) + m = (-m) + m + (k + l) = k + l$. Par le lemme 1.3.1(ii), on a $k = l = 0$, d'où $m = n$.
ii) Si $m \leq n$ et $n \leq k$, il existe $p, q \in \mathbb{N}$ tels que $n = m + p$ et $k = n + q$, si bien que $k = (m + p) + q = m + (p + q)$, et comme $p + q \in \mathbb{N}$, on a $m \leq k$.
iii) Si $n \geq 0$, alors par définition il existe $k \in \mathbb{N}$ tel que $0 + k = n$, soit $k = n$, donc $n \in \mathbb{N}$. Inversement, si $n \in \mathbb{N}$ on a $0 + n = n$, donc $0 \leq n$. □

**Remarque 2.1.9.** Par (iii), on a $\mathbb{N} = \mathbb{Z}_+ = \{n \in \mathbb{Z} : n \geq 0\}$. Il s'ensuit qu'on a aussi $\mathbb{Z} - \mathbb{N} = \{n \in \mathbb{Z} : n < 0\}$. Ainsi, si $n$ est un entier relatif, on a soit $n < 0$, soit $n = 0$, soit $n > 0$.

En outre, la définition de l'ordre naturel par l'addition permet d'établir les relations suivantes entre les deux :

**Proposition 2.1.10.** *Soient* $m, n, k$ *trois entiers relatifs.*
*i) Si* $m \leq n$*, alors* $m + k \leq n + k$.
*ii) Si* $m < n$*, alors* $m + k < n + k$.
*iii) On a* $m \leq n$ *si et seulement si* $n - m \in \mathbb{N}$.

*Démonstration.* i) Si $m \leq n$, par définition il existe $p \in \mathbb{N}$ tel que $m + p = n$, d'où $(m + k) + p = m + (k + p) = m + (p + k) = (m + p) + k$ (par les propriétés de l'addition) $= n + k$; autrement dit, on a $m + k \leq n + k$.
ii) En exercice.
iii) Supposons que $m \leq n$ : par (i), on a $0 = m - m = m + (-m) \leq n + (-m) = n - m$, donc $n - m \in \mathbb{N}$ par 2.1.8(iii). Inversement, si $n - m \in \mathbb{N}$, on a $0 \leq n - m$, d'où $m = 0 + m \leq (n - m) + m$ (par (i)) $= n$. □

L'axiome 2.1.4 se reformule sous la forme de la propriété de trichotomie suivante, déjà évoquée à propos de l'ensemble $\mathbb{N}$ (Proposition 1.3.8), et qui reflète le caractère "total" de l'ordre naturel :

**Proposition 2.1.11.** *Soient $m$ et $n$ deux entiers relatifs. Alors un et un seul des cas suivants est vérifié :*
*i)* $m < n$
*ii)* $m = n$
*iii)* $m > n$.

*Démonstration.* Il s'agit d'une simple reformulation de la remarque 2.1.9, en remarquant que $m < n$ si et seulement $m - n < 0$, $m = n$ si et seulement si $m - n = 0$ et $m > n$ si et seulement si $m - n > 0$. □

### Exercices de la section

*Exercice* 2.1.12. i) Démontrer que le seul entier relatif $n$ tel que $n = -n$ est 0. Indication : raisonner par contraposée en supposant que $n \neq 0$, et distinguer les cas, selon que $n \in \mathbb{N}$ ou $n \notin \mathbb{N}$.
ii) Supposons que $m, n, k \in \mathbb{Z}$ et que $m < n$. Montrer que $m+k < n+k$ (proposition 2.1.10(ii)). En déduire que si $m \leq n$, alors $m + k \leq n + k$.
iii) Démontrer la deuxième partie de la remarque 2.1.9, et en déduire la proposition 2.1.11 (compléter la démonstration).

## 2.2 La multiplication et la divisibilité dans $\mathbb{Z}$

### 2.2.1 Définition algébrique de la multiplication

Une fois que nous disposons d'une description rigoureuse de l'addition et de la soustraction des entiers relatifs, ainsi que de leurs propriétés élémentaires, nous pouvons *définir* rigoureusement leur multiplication.
Pour cela, nous partons d'une propriété essentielle que doit posséder la multiplication : si $a, b, c, d$ sont des entiers *relatifs*, nous devrions avoir l'égalité $(a - b) \times (c - d) = ac + bd - ad - bc = (ac + bd) - (ad + bc)$, en développant le produit et par les règles intuitives du calcul. Dans l'expression au membre de droite, on voit apparaître la différence de deux nombres, soit une expression de la même forme que les deux expressions multipliées au membre de gauche.
En utilisant la représentation d'un entier relatif $n$ comme différence de deux entiers naturels, évoquée dans la section 2.1, nous pouvons poser la définition suivante, qui prend en compte les différentes représentations possibles :

**Définition 2.2.1.** Si $n$ et $m$ sont deux entiers relatifs tels que $n = a-b$ et $m = c-d$, pour $a, b, c, d \in \mathbb{N}$, le *produit de $n$ et $m$*, noté $n \times m$, $n.m$ ou $nm$, est le nombre entier relatif $(ac + bd) - (ad + bc)$. L'application qui associe à $(n, m) \in \mathbb{Z} \times \mathbb{Z}$ le produit $n.m \in \mathbb{Z}$ est la *multiplication* des entiers relatifs.

Un problème évident surgit immédiatement avec cette définition. En effet, celle-ci dépend d'une *représentation* des deux facteurs $n$ et $m$ comme différences d'entiers.

Or, puisqu'il existe toujours une infinité de telles représentations pour chaque entier relatif, si nous choisissons d'autres représentations, disons $n = a' - b'$ et $m = c' - d'$, le résultat prévu, c'est-à-dire $(a'c' + b'd') - (a'd' + b'c')$, est *a priori* différent. Dans ce genre de situation, il faut donc vérifier que la définition *ne dépend pas* du choix de la représentation :

**Lemme 2.2.2.** *La multiplication des entiers relatifs est bien définie : si* $n = a-b = a'-b'$ *et* $m = c-d = c'-d'$*, alors on a* $(ac+bd)-(ad+bc) = (a'c'+b'd')-(a'd'+b'c')$.

*Démonstration.* Reformulons les hypothèses : de $a-b = a'-b'$, on tire $a+b' = a'+b$, et de $c - d = c' - d'$ on tire $c + d' = c' + d$. Nous voulons alors démontrer que $(ac+bd)+(a'd'+b'c') = (ad+bc)+(a'c'+b'd')$. Ces clauses ne portent plus désormais que sur l'ensemble $\mathbb{N}$ des entiers naturels, dont nous allons utiliser les propriétés pour démontrer la dernière, à partir des deux premières, en deux étapes. On a d'abord $ac + bd + a'd + b'c = (a + b')c + (b + a')d$ (en factorisant) $= (a' + b)c + (a + b')d$ (puisque $a + b' = a' + b$) $= a'c + bc + ad + b'd = ad + bc + a'c + b'd$, ce qui donne une première égalité intermédiaire. Ensuite, en utilisant la même idée on a $a'c + b'd + a'd' + b'c' = a'(c + d') + b'(d + c') = a'(c' + d) + b'(d' + c)$ (puisque $c + d' = c' + d$) $= a'c' + a'd + b'd' + b'c = a'd + b'c + a'c' + b'd'$, ce qui fournit la seconde égalité. En combinant ces deux égalités, c'est-à-dire :

$$\begin{aligned}(ac + bd) + (a'd + b'c) &= (ad + bc) + (a'c + b'd)\\ (a'c + b'd) + (a'd' + b'c') &= (a'd + b'c) + (a'c' + b'd')\end{aligned}$$

en ajoutant $a'd' + b'c'$ à la première, on obtient $(ac+bd)+(a'd+b'c)+(a'd'+b'c') = (ad+bc)+(a'c+b'd)+(a'd'+b'c') = (ad+bc)+(a'd+b'c)+(a'c'+b'd')$, et en simplifiant par $(a'd + b'c)$ grâce au lemme 1.3.1, on a finalement $(ac + bd) + (a'd' + b'c') = (ad + bc) + (a'c' + b'd')$, ce qu'il fallait démontrer. □

**Remarque 2.2.3.** Même si nous avons fait appel à l'intuition du comportement de la soustraction par rapport à la multiplication pour définir celle-ci, nous n'avons utilisé dans la démonstration du lemme que l'addition et la multiplication des entiers *naturels* et la soustraction des entiers relatifs.

**Exemple 2.2.4.** Vérifions la multiplication de deux nombres entiers relatifs à partir de deux représentations arbitraires : on a par exemple $-13 = 7 - 20$ et $-204 = 78-282$. Il vient $(7-20).(78-282) = (7.78+20.282)-(7.282+20.78) = 6186-3534 = 2652$, ce qui est bien le résultat qu'on voulait obtenir (puisque $13.204 = 2652$). Bien sûr, en général on utilise les représentations les plus simples : si $n \in \mathbb{N}$, on écrit $n = n - 0$, et si $n \notin \mathbb{N}$, comme $-n \in \mathbb{N}$ on écrit $n = 0 - (-n)$.

La figure 8 donne une représentation géométrique de la multiplication des entiers relatifs, valable aussi pour les nombres réels.

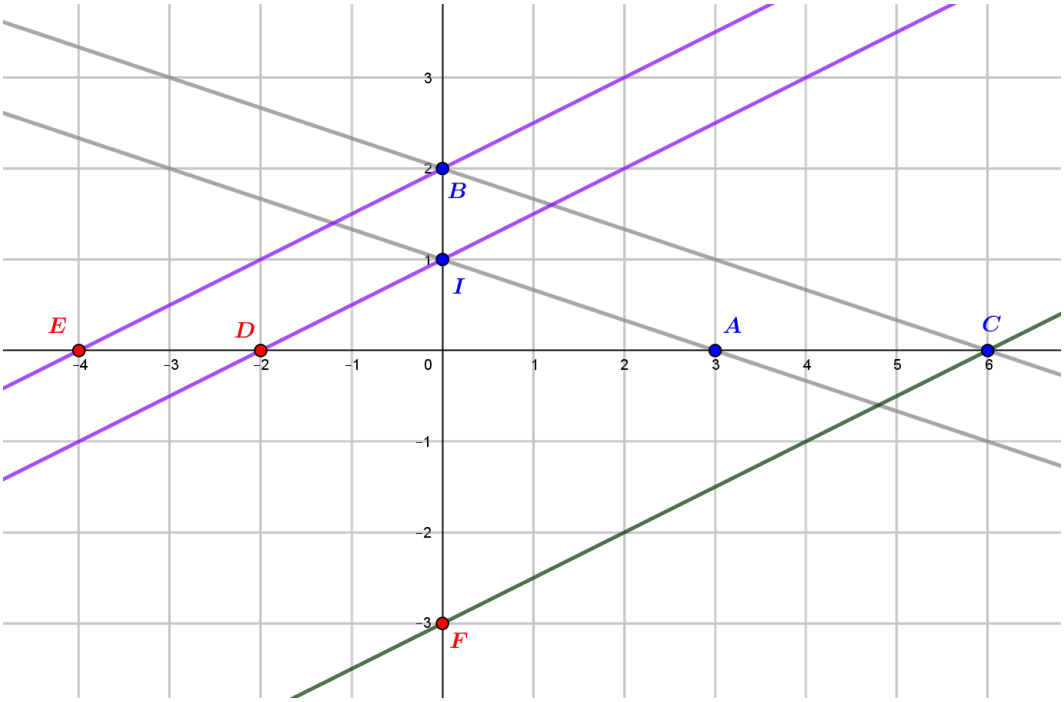



Figure 8: Représentation géométrique du produit d'entiers relatifs. Pour multiplier 3 par 2, on reporte 3 en abscisses (point $A$) et 2 en ordonnées (point $B$); par le théorème de Thalès, le produit $2.3 = 6$ est l'abscisse du point d'intersection $C$ de la parallèle à la droite $(IA)$ passant par $B$ avec l'axe des abscisses. La construction fonctionne pour toutes les combinaisons de signes : $(-2).2 = -4$ (points $D$, $B$ et $E$), et $(-2).(-3) = 6$ (points $D$, $F$ et $C$).

Cette définition de la multiplication peut paraître un peu sophistiquée, et il est possible d'en choisir une autre, utilisant par exemple la valeur absolue, que nous aborderons plus avant. Toutefois, elle rend transparent l'usage de la multiplication des entiers relatifs, et s'avère être plus simple pour en démontrer les propriétés. C'est d'ailleurs cette idée que nous utiliserons au semestre II pour donner une *construction* de l'ensemble $\mathbb{Z}$.
Nous avons ici encore fait l'abus de notation qui consiste à utiliser les mêmes symboles pour le produit dans $\mathbb{N}$ et dans $\mathbb{Z}$; il faut pour le justifier montrer que les deux opérations coïncident sur $\mathbb{N}$. Soient en effet $n$ et $m$ deux entiers *naturels* : puisque $n = n - 0$ et $m = m - 0$ sont deux représentations de $n$ et $m$ comme différences d'entiers naturels, par définition leur produit en tant qu'entiers *relatifs* est le nombre $(n.m + 0.0) - (n.0 + 0.m) = n.m$, soit leur produit en tant qu'entiers *naturels*.

### 2.2.2 Propriétés de la multiplication

A partir de cette définition purement "algébrique", nous pouvons retrouver les propriétés élémentaires de la multiplication des nombres entiers relatifs, évoquées dans le premier cours, à partir des seules propriétés de l'addition et de la multiplication des entiers naturels.

**Proposition 2.2.5.** *Si $m, n, k$ sont trois entiers relatifs, on a :*
*o)* $0 \times m = 0$ *(0 est élément absorbant de la multiplication)*

*i)* $1 \times m = m$ *(*$1$ *est élément neutre de la multiplication)*
*ii)* $m \times n = n \times m$ *(la multiplication est commutative)*
*iii)* $m \times (n \times k) = (m \times n) \times k$ *(la multiplication est associative)*
*iv)* $m \times (n+k) = (m \times n) + (m \times k)$ *(la multiplication est distributive sur l'addition).*

*Démonstration.* Choisissons trois représentations $m = a - b$, $n = c - d$ et $p = e - f$ des trois nombres de l'énoncé comme différences d'entiers naturels, et appliquons les propriétés de la proposition 1.2.5 à partir de la définition de la multiplication dans $\mathbb{Z}$.
o) On a $0.m = (0-0).(a-b) = (0.a + 0.b) - (0.b + 0.a) = 0 - 0 = 0$.
i) On a $1.m = (1-0).(a-b) = (1.a + 0.b) - (1.b + 0.a) = a - b = m$.
ii) On a $n.m = (c-d).(a-b) = (ca + db) - (cb + da) = (ac + bd) - (bc + ad)$ (par commutativité de $\times$ dans $\mathbb{N}$) $= (a-b).(c-d) = m.n$.
iii) On a $m.(n.p) = (a-b).((c-d).(e-f)) = (a-b).((ce+df)-(cf+de)) = (ace+adf+bcf+bde)-(acf+ade+bce+bdf)$ en utilisant notamment l'associativité de la multiplication dans $\mathbb{N}$. De même, on a $(m.n).p = ((ac+bd)-(ad+bc)).(e-f) = (ace+bde+adf+bcf)-(acf+bdf+ade+bce)$, et en utilisant les propriétés de l'addition dans $\mathbb{N}$, on s'aperçoit que les deux résultats sont identiques.
iv) On a $m \times (n+p) = (a-b).((c-d)+(e-f)) = (a-b).((c+e)-(d+f)) = (a(c+e)+b(d+f))-(a(d+f)+b(c+e)) = (ac+ae+bd+bf)-(ad+af+bc+be)$ (par distributivité de $\times$ sur $+$ dans $\mathbb{N}$) $= ((ac+bd)-(ad+bc))+((ae+bf)-(af+be)) = ((a-b).(c-d))+((a-b).(e-f)) = m \times n + m \times p$, ce qu'il fallait démontrer. □

La multiplication des nombres entiers relatifs possède en outre la propriété suivante, dite *d'intégrité*, très importante en algèbre.

**Théorème 2.2.6.** *Si* $m, n \in \mathbb{Z}$ *et* $m \times n = 0$*, alors* $m = 0$ *ou* $n = 0$.

*Démonstration.* Ecrivons $m = (a-b)$ et $n = (c-d)$ avec $a, b, c, d \in \mathbb{N}$ et supposons que $0 = m \times n = (a-b) \times (c-d) = (ad+bc) - (bd+ac)$ : autrement dit, on a $ad + bc = bd + ac$. Supposons que $m = a - b \neq 0$ : on a donc $a \neq b$, par exemple $a < b$, et il existe alors $x \in \mathbb{N}^*$ tel que $b = a + x$. Il vient $ad + ac + xc = ad + bc = bd + ac = ad + xd + ac = ad + ac + xd$. Par la simplifiabilité de l'addition dans $\mathbb{N}$ (lemme 1.3.1), on en déduit que $xc = xd$, et comme $x \neq 0$, par la proposition 1.2.7 que $c = d$, soit $n = (c-d) = 0$. Le cas où $b < a$ se traite de la même manière, et le théorème est démontré. □

**Remarque 2.2.7.** i) Cette propriété s'utilise souvent sous sa forme contraposée : si $m, n \in \mathbb{Z}$ et $m$ et $n$ sont non nuls, alors le produit $mn$ est non nul.
ii) On peut aussi démontrer cette propriété en utilisant la caractérisation du produit dans $\mathbb{Z}$ à partir de la valeur absolue (proposition 2.3.3).

Le rapport entre la multiplication et la soustraction des entiers relatifs est essentiellement exprimé par la propriété suivante :

**Proposition 2.2.8.** *Si* $n$ *est un entier relatif, alors* $(-1).n = -n$.

*Démonstration.* On a $-1 = 0 - 1$, si bien qu'en écrivant $n = a - b$ pour $a, b \in \mathbb{N}$, on a $(-1).n = (0-1).(a-b) = (0.a+1.b)-(0.b+1.a) = b - a = -n$ par la proposition 2.1.5. □

Puisque les entiers relatifs ont un signe, positif ou négatif, le rapport entre la multiplication et l'ordre naturel dans $\mathbb{Z}$ est plus subtil que dans $\mathbb{N}$ : il faut faire attention à ce que le signe d'un facteur "change le sens des inégalités" :

**Proposition 2.2.9.** *Soient $m, n$ et $k$ trois entiers relatifs.*
*i) Si $m < n$ et $k > 0$, on a $m.k < n.k$*
*ii) Si $m < n$ et $k < 0$, on a $m.k > n.k$*
*iii) Si $m \leq n$ et $k \geq 0$, on a $m.k \leq n.k$*
*iv) Si $m \leq n$ et $k \leq 0$, on a $m.k \geq n.k$.*

*Démonstration.* La démonstration est laissée à l'étudiant(e) (voir les exercices). □

### 2.2.3 Divisibilité et division euclidienne dans $\mathbb{Z}$

Nous définissons la relation de divisibilité comme dans le cours n° 1, exactement de la même manière que nous l'avons définie dans $\mathbb{N}$.

**Définition 2.2.10.** Soient $m$ et $n$ deux entiers relatifs.
i) On dit que $m$ *divise* $n$, ce qu'on note $m|n$, si il existe $k \in \mathbb{Z}$ tel que $n = m \times k$. Dans ce cas, on dit aussi que $m$ est un *diviseur de* $n$ et que $n$ est un *multiple de* $m$.
ii) Si $m$ n'est pas nul et $m|n$, l'unique entier relatif $k$ tel que $n = k.m$ est appelé le *quotient* de $n$ par $m$.

**Remarque 2.2.11.** L'entier relatif $k$ de la clause (ii) est unique par intégrité (2.2.6). En effet, si il existe $k' \in \mathbb{Z}$ tel que $n = k'.m$, on a alors $k'.m = k.m$, d'où $(k'-k).m = 0$, et comme $m \neq 0$, on en déduit $k - k' = 0$, soit $k = k'$.

**Exemple 2.2.12.** L'entier $-17$ divise l'entier 221, puisqu'on a $(-17).(-13) = 221$. L'entier 24 ne divise pas $-354$, car sinon il existerait $k \in \mathbb{Z}$ tel que $24.k = -354$ : on aurait alors $k \leq -15$ (si $k > -15$, on a $k \geq -14$, d'où $24.k \geq 24.(-14) = -336$ par l'exercice 2.2.18(ii)), mais pour $k \leq -15$ on a $24.k \leq 24.(-15) = -360$.

Les propriétés élémentaires de la relation de divisibilité sont quasiment identiques à celles de sa restriction à $\mathbb{N}$, à l'exception de l'anti-symétrie (voir la proposition 1.3.15).

**Proposition 2.2.13.** *Soient $m, n, p \in \mathbb{Z}$. On a les propriétés suivantes :*
*o) $1|m$ et $m|0$*
*i) $m|m$ (la relation $|$ est réflexive)*
*ii) si $m|n$ et $n|p$, alors $m|p$ (la relation $|$ est transitive)*
*iii) si $m|n$ et $n|m$, alors $m = n$ ou $m = -n$.*

*Démonstration.* Laissée en exercice à l'étudiant(e) (reprendre la preuve de la proposition 1.3.15). □

En général, pour $m$ et $n$ deux entiers relatifs et $n \neq 0$, il n'est possible de former le quotient $m/n$ que si $n$ divise $m$. Dans le cas général, la division est "incomplète", et il demeure un "reste", comme dans le cas des entiers naturels (section 1.4).
On formule précisément cette idée à travers l'extension de la *division euclidienne* de l'ensemble $\mathbb{N}$ à l'ensemble $\mathbb{Z}$, sous la forme suivante, déjà démontrée au chapitre 5 du cours n° 1.

**Théorème 2.2.14.** *Si $a$ et $b$ sont deux entiers relatifs tels que $b > 0$, alors il existe des entiers relatifs $q$ et $r$ uniques tels que $a = bq + r$ et $0 \leq r < b$.*

*Démonstration.* Distinguons deux cas, selon que $a \in \mathbb{N}$ ou bien que $a \in \mathbb{Z} - \mathbb{N}$. Si $a \in \mathbb{N}$, la conclusion de l'énoncé découle de la division euclidienne des entiers naturels (théorème 1.4.5). Si $a < 0$, démontrons d'abord l'existence de $q$ et $r$. Effectuons la division euclidienne de $-a$ par $b$, puisque $-a \in \mathbb{N}$ : il existe des entiers naturels uniques $q_0$ et $r_0$ tels que $-a = bq_0 + r_0$ et $0 \leq r_0 < b$. On peut donc écrire, en multipliant par $-1$, $a = -bq_0 - r_0$. Distinguons à nouveau deux cas, selon que $r_0 = 0$ ou non. Si $r_0 = 0$, alors on a $a = b.(-q_0)$, donc $q = -q_0$ et $r = 0$ conviennent. Si $r_0 > 0$, $-r_0$ ne peut pas être un reste, mais comme $r_0 < b$ on peut écrire à la place de l'égalité précédente $a = -bq_0 - b + b - r_0 = b(-q_0 + 1) + (b - r_0)$. Comme $-b < -r_0 < 0$ par les propriétés des inégalités (on a multiplié l'inégalité $0 < r_0 < b$ par $-1$), il vient $0 = b - b < b - r_0 < b$, si bien que $q = -q_0 + 1$ et $r = b - r_0$ conviennent. Par disjonction des cas, l'existence de $q$ et $r$ est démontrée pour $a < 0$. L'unicité de $q$ et $r$ se démontre alors exactement comme dans le théorème 1.4.5; par disjonction des cas, le théorème est démontré. □

**Exemple 2.2.15.** On a $-73 = 8.(-10) + 7$, et comme $0 \leq 7 < 8$, $-10$ est le quotient, et 7 est le reste, de la division euclidienne de $-73$ par 8. Or, on a aussi $73 = 8.9 + 1$, donc 9 est le quotient, et 1 est le reste, de la division euclidienne de 73 par 8 : si $b > 0$, on n'obtient pas en général le quotient de la division euclidienne de $-a$ par $b$ comme l'opposé du quotient de la division de $a$ par $b$.

**Corollaire 2.2.16.** *Si $m$ et $n$ sont deux entiers relatifs et $n > 0$, on a $n|m$ si et seulement si le reste dans la division euclidienne de $m$ par $n$ est nul.*

*Démonstration.* Supposons que $n|m$ : il existe $k \in \mathbb{Z}$ tel que $m = n.k+0$ : par unicité du quotient et du reste dans la division euclidienne de $m$ par $n$, on a donc $r = 0$. Réciproquement, écrivons cette division euclidienne sous la forme $m = n.q + r$, avec $0 \leq r < n$ : si $r = 0$, on a $m = n.q$, si bien que $n|m$. □

**Remarque 2.2.17.** Ce critère permet de déterminer lorsqu'un entier relatif $n$ non nul quelconque divise un entier relatif $m$. En effet, si $n < 0$, on a $n|m$ si et seulement si $-n|m$, et on applique alors le corollaire.

L'étude de la relation de divisibilité constitue en quelque sorte l'arithmétique des nombres entiers relatifs, à laquelle nous nous consacrerons jusqu'à la fin de chapitre, après avoir traité de la valeur absolue.

## Exercices de la section

*Exercice* 2.2.18. i) Démontrer que la multiplication est distributive sur la soustraction dans $\mathbb{Z}$, autrement dit que pour tous $m, n, p \in \mathbb{Z}$, on a $m.(n - p) = mn - mp$.
ii) Démontrer la proposition 2.2.9.
iii) Montrer que pour tout $m \in \mathbb{Z}$, on a $m^2 \in \mathbb{N}$, c'est-à-dire $m^2 \geq 0$.
iv) Démontrer la proposition 2.2.13.
v) En utilisant les idées du théorème 2.2.14, effectuer les divisions euclidiennes de $-167$ par 9, de $-344$ par 27.

## 2.3 La valeur absolue dans $\mathbb{Z}$

### 2.3.1 Définitions et propriétés de la valeur absolue

Rappelons que par la proposition 2.1.10, pour $m, n \in \mathbb{Z}$ on a $m \leq n$ si et seulement si $n - m \in \mathbb{N}$, et que par la proposition 2.1.11, on a soit $m < n$, soit $m = n$, soit $m > n$, et que ces trois cas sont mutuellement exclusifs, cette propriété étant déduite de l'ordre naturel dans $\mathbb{N}$.
Nous pouvons à partir de là définir rigoureusement la *valeur absolue* d'un entier relatif $n$, c'est-à-dire la "magnitude" de $n$, puisque pour $m = 0$, on a soit $n < 0$, soit $n = 0$, soit $n > 0$, ou du point de vue de l'ordre large, $n \geq 0$ ou $n \leq 0$ (c'est-à-dire $-n \geq 0$), ce qui est en somme une traduction de l'axiome 2.1.4. On pose alors la définition habituelle suivante :

**Définition 2.3.1.** Si $n$ est un entier relatif, la *valeur absolue de* $n$ est définie par disjonction des cas comme l'entier naturel $|n|$ tel que :
i) $|n| = n$ si $n \in \mathbb{Z}_+ = \mathbb{N}$, c'est-à-dire si $n \geq 0$
ii) $|n| = -n$ si $n \in \mathbb{Z}_-$, c'est-à-dire si $n \leq 0$.

**Remarque 2.3.2.** o) Dans le cas où $n = 0$, les deux définitions conviennent.
ii) La valeur absolue est une application $|.| : \mathbb{Z} \to \mathbb{N}$.

La figure 9 donne l'allure de la fonction valeur absolue sur quelques entiers relatifs.

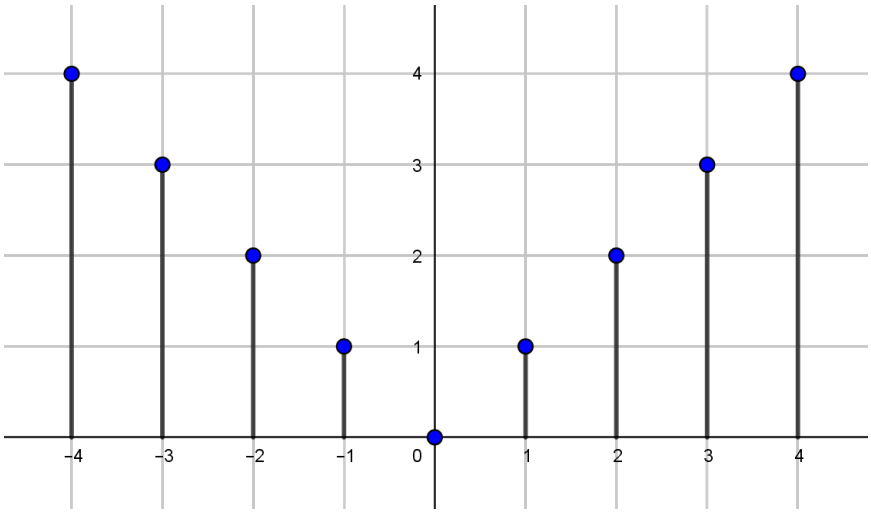



Figure 9: La valeur absolue d'un entier relatif représente sa "magnitude", en faisant abstraction de son signe.

La valeur absolue permet de donner une caractérisation directe de la multiplication des entiers relatifs à partir de celle des entiers naturels :

**Proposition 2.3.3.** *Soient $m$ et $n$ deux nombres entiers relatifs.*
*i) Si $m$ et $n$ ont même signe (c'est-à-dire si $m, n \geq 0$ ou $m, n \leq 0$), alors on a $m.n = |m|.|n|$*
*ii) Si $m$ et $n$ sont de signes contraires (c'est-à-dire si $m \geq 0$ et $n \leq 0$, ou bien si $m \leq 0$ et $n \geq 0$), alors on a $m.n = -|m|.|n|$.*

*Démonstration.* i) Si $m, n \geq 0$, on a $|m| = m$ et $|n| = n$, si bien que $m.n = |m|.|n|$. Si $m, n \leq 0$, on a $|m| = -m$ et $|n| = -n$, si bien que $|m|.|n| = (-m).(-n) = ((-1).m).((-1).n) = ((-1).(-1)).(m.n)$ (par les propriétés de la multiplication) $= m.n$ puisque $(-1).(-1) = 1$.
ii) Si $m \geq 0$ et $n \leq 0$, on a $|m| = m$ et $|n| = -n$, d'où $|m|.|n| = m.(-n) = m.((-1).n) = (-1).(m.n) = -m.n$, d'où $m.n = -|m|.|n|$. Le cas où $m \leq 0$ et $n \geq 0$ se traite de la même manière. □

Les propriétés fondamentales de la valeur absolue, que nous retrouverons dans son prolongement à $\mathbb{Q}$ et à $\mathbb{R}$, sont les suivantes :

**Proposition 2.3.4.** *Soient $m$ et $n$ deux entiers relatifs.*
*i) On a $|m| = 0$ si et seulement si $m = 0$.*
*ii) On a $|m.n| = |m|.|n|$.*
*iii) On a $|m + n| \leq |m| + |n|$ (inégalité triangulaire).*

*Démonstration.* i) Par définition, on a $|0| = 0$, donc supposons inversement que $|m| = 0$ : si $m \geq 0$, on a $m = |m| = 0$, tandis que si $m \leq 0$, on a $m = -|m| = -0 = 0$ donc dans les deux cas, on a $m = 0$.
ii) Distinguons à nouveau les cas selon le signe de $m$ et $n$. Si $m, n \geq 0$, on a $m.n \geq 0$, d'où $|m|.|n| = m.n = |m.n|$; si $m, n \leq 0$, on a $|m|.|n| = m.n$ (par la proposition 2.3.3) $= |m.n|$, puisque $m.n \geq 0$ (par l'exercice 2.2.18(ii)). Si $m \geq 0$ et $n \leq 0$, on a $|m|.|n| = -m.n$ (par la proposition 2.3.3) $= (-1).(m.n) = m.((-1).n)$ (par les propriétés de la multiplication) $= m.(-n) = |m|.|n|$; le cas où $m \leq 0$ et $n \geq 0$ se traite de la même manière.
iii) Distinguons à nouveau les cas. Si $m, n \geq 0$, on a $m + n \geq 0$, donc $|m + n| = m + n = |m| + |n|$, d'où l'inégalité; de même, si $m, n \leq 0$, on a $m + n \leq 0$, donc $|m + n| = -(m + n) = -m - n = |m| + |n|$, d'où l'inégalité. Supposons que $m \geq 0$ et que $n \leq 0$ et distinguons deux cas à l'intérieur de ce cas : si $m + n \geq 0$, on a $|m + n| = m + n \leq m + (-n)$ (puisque $n \leq 0$ et donc $0 \leq -n$ par 2.2.9) $= |m| + |n|$; tandis que si $m + n \leq 0$, on a $|m + n| = -(m + n) = -m - n \leq m + (-n)$ (puisque $m \geq 0$, donc $-m \leq 0$) $= |m| + |n|$, et l'inégalité est démontrée dans les deux sous-cas. Le cas où $m \leq 0$ et $n \geq 0$ se traite de la même manière que le troisième cas. □

**Remarque 2.3.5.** i) Dans le cas où $m$ et $n$ sont de même signe, l'inégalité triangulaire est une égalité.
ii) Comme nous le verrons dans la suite, la valeur absolue joue un rôle essentielle pour associer l'arithmétique dans $\mathbb{Z}$ à l'arithmétique dans $\mathbb{N}$.

### 2.3.2 Minimum et maximum

La proposition 2.1.11 énonce que le prolongement de l'ordre naturel de $\mathbb{N}$ à $\mathbb{Z}$ est encore un ordre total. Ceci signifie que nous pouvons aussi prolonger les notions de minimum et de maximum, évoquées à la section 1.3.2. Cette prolongation sera utile pour aborder certaines questions arithmétiques à partir de la décomposition des entiers en nombres premiers (théorèmes 2.5.7 et 2.5.10).

**Définition 2.3.6.** Soient $m$ et $n$ deux entiers relatifs.
i) Le *minimum* de $m$ et $n$, noté $\min\{m, n\}$, est le plus petit des entiers $m$ et $n$, soit

$m$ si $m \leq n$, ou $n$ si $n < m$.
ii) Le *maximum* de $m$ et $n$, noté $\max\{m, n\}$, est le plus grand des entiers $m$ et $n$, soit $m$ si $n \leq m$, ou $n$ si $m < n$.

Le minimum et le maximum de deux entiers relatifs possèdent des propriétés analogues à celles de ces opérations appliquées aux entiers naturels (proposition 1.3.11). Il faut toutefois faire attention au signe des entiers relatifs impliqués dans ces propriétés, puisque la multiplication par un nombre négatif "renverse le sens des inégalités".

**Lemme 2.3.7.** *Soient $m$ et $n$ sont deux entiers relatifs.*
*i) Si $m < n$, on a $-n < -m$.*
*ii) On a $\min\{-m, -n\} = -\max\{m, n\}$ et $\max\{-m, -n\} = -\min\{m, n\}$.*

*Démonstration.* i) Il s'agit d'une application directe de la proposition 2.2.9, avec $k = -1 < 0$.
ii) Distinguons deux cas, selon que $m \leq n$ ou $n \leq m$. Si $m \leq n$, par (i) on a $-n \leq -m$ (si $m = n$, on a bien sûr $-n \leq -m$), donc $\min\{-m, -n\} = -n$, tandis que $\max\{m, n\} = n$, d'où la première égalité. On a également $\max\{-m, -n\} = -m = -\min\{m, n\}$, ce qui est la seconde égalité. En échangeant le rôle de $m$ et $n$, on obtient directement les deux égalités dans l'autre cas, et le lemme est démontré. □

Ainsi, la multiplication par $-1$ "échange" les opérations de minimum et de maximum dans $\mathbb{Z}$. Ceci permet d'affiner la description de leurs propriétés :

**Proposition 2.3.8.** *Si $m, n$ et $k$ sont trois entiers relatifs, on a :*
*i) $m = n$ si et seulement si $\min\{m, n\} = \max\{m, n\}$*
*ii) $m \leq n$ si et seulement $\min\{m, n\} = m$, si et seulement $\max\{m, n\} = n$*
*iii) $m + \min\{n, k\} = \min\{m + n, m + k\}$ et $m + \max\{n, k\} = \max\{m + n, m + k\}$*
*iv) $m \times \min\{n, k\} = \min\{m \times n, m \times k\}$ et $m \times \max\{n, k\} = \max\{m \times n, m \times k\}$ si $m \geq 0$*
*v) $m \times \min\{n, k\} = \max\{m \times n, m \times k\}$ et $m \times \max\{n, k\} = \min\{m \times n, m \times k\}$ si $m \leq 0$.*

*Démonstration.* Comme pour la proposition 1.3.11, la démonstration est laissée à l'étudiant(e), à l'exception de la clause (v), que nous traitons à cause de la question du signe. Si $m \leq 0$, on a $-m \geq 0$, d'où $m \times \min\{n, k\} = -|m|.\min\{n, k\} = |m|.\max\{-n, -k\}$ (par le lemme 2.3.7) $= \max\{-|m|.n, -|m|, k\}$ (par la clause (iv)) $= \max\{m.n, m.k\}$. De même, on a $m \times \max\{n, k\} = -|m|.\max\{n, k\} = -\max\{|m|.n, |m|.k\}$ (par la clause (iv)) $= \min\{-|m|.n, -|m|.k\}$ (par le lemme 2.3.7) $= \min\{m.n, m.k\}$, et la seconde égalité est démontrée. □

**Exemple 2.3.9.** On a bien $-63 = \min\{-42, -63\} = (-7).\max\{6, 9\}$ et $-88 = \max\{-88, -132\} = (-11).\min\{8, 12\}$.

**Remarque 2.3.10.** A cause de la distributivité de l'addition sur le min ou le max (clause (iii) de la proposition 2.3.8), dans les mathématiques dites "tropicales" on considère parfois l'addition comme une "multiplication" et le max (ou le min) comme une "addition" !

### Exercices de la section

*Exercice* 2.3.11. Démontrer le théorème 2.2.6 à partir de la proposition 1.2.7 et de la caractérisation de la mutliplication dans $\mathbb{Z}$ par la valeur absolue (proposition 2.3.3).

## 2.4 Nombres premiers entre eux

Dans la section 1.6, nous avons introduit le *plus grand commun diviseur* de deux nombres entiers *naturels*, et la notion de nombres entiers naturels *premiers entre eux*.
Si l'algorithme d'Euclide nous a donné le moyen de "calculer" théoriquement le p.g.c.d de deux nombres entiers naturels, nous n'avons pas approfondi la question de comment déterminer théoriquement si deux nombres entiers naturels sont premiers entre eux. L'algorithme d'Euclide nous donne un moyen pratique (calculer le p.g.c.d !) mais il existe un critère théorique fondamental, le théorème de Bézout.
La raison pour laquelle nous avons reporté cette question ici, est que l'étude de la "primalité relative" est plus naturelle dans le contexte de l'ensemble $\mathbb{Z}$ des nombres entiers relatifs, même en ce qui concerne les entiers naturels. En fait, le théorème de Bézout s'énonce à partir des nombres entiers relatifs, même si l'on ne considère que des entiers naturels.
Nous reprenons donc ici l'étude des nombres premiers entre eux pour l'approfondir, en étendant les définitions adéquates déjà introduites pour les entiers naturels.
Nous commençons l'arithmétique des entiers relatifs par cette question, car elle nous permettra d'avancer sur la théorie des nombres premiers, où nous démontrerons le théorème de Gauss sur la décomposition en nombres premiers, grâce au lemme d'Euclide.

**Définition 2.4.1.** i) Si $m$ et $n$ sont deux entiers relatifs non tous deux nuls, le *plus grand commun diviseur de $m$ et $n$* est le p.g.c.d de $|m|$ et $|n|$. On le note aussi $pgcd(m,n)$ ou encore $m \wedge n$.
ii) On dit que deux entiers relatifs $m$ et $n$ sont *premiers entre eux*, si $m \wedge n = 1$.

**Remarque 2.4.2.** o) Le p.g.c.d de deux entiers relatifs $m$ et $n$ quelconques est donc toujours un entier naturel.
i) Cette définition est encore parfaitement analogue à la définition introduite pour les entiers naturels : le p.g.c.d des entiers relatifs $m$ et $n$ est ici encore le plus grand entier relatif $d$ tel que $d$ divise à la fois $m$ et $n$ (voir les exercices).
ii) Nous verrons dans cette section que le p.g.c.d de $m$ et $n$ est également *un* plus grand diviseur commun de $m$ et $n$ au sens de la divisibilité. Autrement dit, on a $m \wedge n | m, n$, et si $d \in \mathbb{Z}$ divise à la fois $m$ et $n$, alors $d$ divise $m \wedge n$. Or, cette propriété est également vraie de $-m \wedge n$, si bien que sur le plan de la divisibilité, l'ordre naturel dans $\mathbb{Z}$ n'est pas très pertinent : nous aurions pu définir *un* p.g.c.d de $m$ et $n$ comme *un* entier relatif ayant cette propriété. Comme il n'existe que deux tels entiers relatifs, on choisit le plus grand pour l'ordre naturel, c'est-à-dire celui qui est positif.

Voici le critère fondamental de primalité relative entre deux nombres entiers relatifs, que nous démontrons à l'aide de l'algorithme d'Euclide sur les nombres entiers

naturels.

**Théorème 2.4.3** (Théorème de Bézout)**.** *Si $m$ et $n$ sont deux entiers relatifs non nuls, alors il existe deux entiers relatifs $u$ et $v$ tels que $pgcd(m,n) = mu + nv$.*

*Démonstration.* Supposons d'abord que $m, n \in \mathbb{N}$. On a soit $n \leq m$ soit $m \leq n$, et dans les deux cas on a $pgcd(m,n) = pgcd(n,m)$, donc quitte à intervertir $m$ et $n$ si nécessaire on peut supposer que $n \leq m$ (l'autre cas est traité de manière similaire), donc $m > 0$. Soit $(r_i)_{\mathbb{N}}$ la suite obtenue à partir de l'algorithme d'Euclide appliqué à $m$ et $n$ (section 1.6). Si $r_1 = 0$, on a $m = nq_1 + r_1 = nq_1$, donc $n|m$ et pour $u = 0$ et $v = 1$, on a bien alors $um + vn = n = pgcd(m,n)$. Si $r_1 \neq 0$, par définition on a $m = nq_1 + r_1$, d'où $r_1 = m + n(-q_1)$ : par la proposition 1.6.10, si $r_2 = 0$ on a $pgcd(m,n) = r_1$, qui est de la forme désirée. Supposons maintenant que $r_2 \neq 0$, et soit $N$ le plus grand entier naturel $i \geq 2$ tel que $r_i \neq 0$, par le lemme 1.6.9. On suppose que pour tout $i = 0, \ldots, N-1$, il existe $u_i, v_i \in \mathbb{Z}$ tels que $r_i = mu_i + nv_i$. Par définition, on peut écrire $r_{N-2} = r_{N-1}q_N + r_N$, d'où $r_N = r_{N-2} - r_{N-1}q_N = mu_{N-2} + nv_{N-2} - q_N(mu_{N-1} + nv_{N-1}) = m(u_{N-2} - q_N u_{N-1}) + n(v_{N-2} - q_N v_{N-1})$, qui est encore de la forme désirée. Par la proposition 1.6.10 à nouveau, on a $r_N = pgcd(m,n)$, d'où le résultat dans ce cas. En général, si $m, n \in \mathbb{Z}$, on a $|m|, |n| \in \mathbb{N}$ : par le cas précédent, il existe $u, v \in \mathbb{Z}$ tels que $pgcd(m,n) = pgcd(|m|,|n|) = |m|u + |n|v$. Par définition de la valeur absolue, il existe donc des entiers relatifs $u', v' \in \mathbb{Z}$ tels que $pgcd(m,n) = mu' + nv'$. En effet, si $|m| = m$ et $|n| = n$, alors $u' = u$ et $v' = v$ conviennent; si $|m| = -m$ et $|n| = n$, alors $u' = -u$ et $v' = v$ conviennent; si $|m| = m$ et $|n| = -n$, alors $u' = u$ et $v' = -v$ conviennent; et si $|m| = -m$ et $|n| = -n$, alors $u' = -u$ et $v' = -v$ conviennent. □

**Remarque 2.4.4.** L'essentiel de la démonstration porte sur le cas où $m, n \in \mathbb{N}$, et l'étude du second cas (où $r_1 \neq 0$) montre que l'introduction des entiers relatifs est essentielle, puisqu'il faut utiliser l'opposition du quotient $q_1$ (dans le cas où $r_2 = 0$) ou une soustraction (dans le cas où $r_2 \neq 0$).

Du théorème de Bézout on tire le critère théorique suivant, qui permet de caractériser les couples $(m,n)$ d'entiers relatifs premiers entre eux :

**Corollaire 2.4.5.** *Deux entiers relatifs non nuls $m$ et $n$ sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que $mu + nv = 1$.*

*Démonstration.* Par le théorème de Bézout 2.4.3, il existe $u, v \in \mathbb{Z}$ tels que $mu + nv = pgcd(m,n)$. Si $m$ et $n$ sont premiers entre eux, alors $pgcd(m,n) = 1$, d'où l'égalité. Inversement, si il existe $u, v \in \mathbb{Z}$ tels que $mu + nv = 1$, notons $d = pgcd(m,n)$ : comme $d$ divise à la fois $m$ et $n$, il divise $mu + nv$, si bien que $d \mid 1$ et finalement, $d = 1$ et $m$ et $n$ sont premiers entre eux. □

Un autre corollaire du théorème de Bézout permet de déterminer quand une équation de la forme $ax + by = c$ possède des solutions entières en $x$ et $y$.

**Corollaire 2.4.6.** *Si $m$, $n$ et $c$ sont trois entiers relatifs et $m$ et $n$ sont non nuls, alors l'équation $mx + ny = c$ possède une solution $(x,y) \in \mathbb{Z}^2$ si et seulement si $m \wedge n | c$.*

*Démonstration.* Supposons que cette équation possède une solution $(u, v) \in \mathbb{Z}^2$, de sorte que l'on a l'égalité $mu + nv = c$ : comme $m \wedge n | m, n$, on a $m \wedge n | mu + nv = c$. Réciproquement, si $m \wedge n | c$ il existe $k \in \mathbb{Z}$ tel que $c = k.(m \wedge n)$; par le théorème de Bézout 2.4.3, soient $u, v \in \mathbb{Z}$ tels que $mu + nv = m \wedge n$ : on a $k.(mu + nv) = k.(m \wedge n) = c$, donc le couple $(ku, kv)$ est une solution de d'équation $mx + ny = c$. □

La démonstration du théorème de Bézout montre qu'ici comme ailleurs, cela n'aurait pas trop de sens de séparer artificiellement l'arithmétique dans l'ensemble $\mathbb{N}$ de l'arithmétique dans l'ensemble $\mathbb{Z}$. Comme le montrera la section suivante, à propos de la décomposition en nombres premiers, il faut plutôt voir la seconde comme un "approfondissement" de la première.
Trouver une *relation de Bézout* entre deux entiers relatifs $m$ et $n$ non nuls, c'est trouver deux entiers relatifs $u$ et $v$ tels que $um + vn = pgcd(m, n)$. En utilisant la stratégie de la seconde partie de la démonstration du théorème de Bézout 2.4.3, il suffit de savoir le faire pour $m, n \in \mathbb{N}$.
Ceci peut se faire grâce à l'algorithme d'Euclide : écrivons le complètement pour deux entiers naturels $m \geq n > 0$ comme dans la section 1.6. Nous définissons alors deux suites $(q_i)$ et $(r_i)$ d'entiers comme suit. On pose $n = r_0$, on écrit $m = nq_0 + r_1$ la division euclidienne de $m$ par $n$ (donc avec $r_1 < n$) et pour tout $n \geq 1$, on définit $q_n$ et $r_{n+1}$ en écrivant la division euclidienne de $r_{n-1}$ par $r_n$ sous la forme $r_{n-1} = r_n q_n + r_{n+1}$ (donc avec $r_{n+1} < r_n$).
Si on note $N$ l'indice du dernier reste non nul (par le lemme 1.6.7), on dispose ainsi de $N$ relations $m = nq_0 + r_1$, $r_0 = n = r_1 q_1 + r_2$, $r_1 = r_2 q_2 + r_3$, ... et $r_{N-2} = r_{N-1} q_{N-1} + r_N$. On en tire $r_1 = m - nq_0$ et $r_2 = n - r_1 q_1 = n - (m - nq_0)q_1 = n(1 + q_0 q_1) + m(-q_1)$, puis $r_3 = r_1 - r_2 q_2$, soit $r_3 = (m - nq_0) - q_2(n(1 + q_0 q_1) + m(-q_1)) = m(1 + q_1 q_2) + n(-q_0).(1 + q_1 q_2)$. De proche en proche, en substituant à $r_n$ la valeur obtenue par l'équation $r_{n-2} = r_{n-1} q_{n-1} + r_n$, soit $r_n = r_{n-2} - r_{n-1} q_{n-1}$, pour $n = 2, \ldots, N$, on obtient une relation de Bézout entre $m$ et $n$.

**Exemple 2.4.7.** Cherchons une relation de Bézout entre 561 et $-381$, en appliquant l'algorithme d'Euclide à $m = 561$ et $n = 385$. On obtient $561 = 385.1 + 176$, $385 = 176.2 + 33$, $176 = 33.5 + 11$ et $33 = 11.3$. On en tire $176 = 561 - 385$ et $33 = 385 - 176.2 = 385 - (561 - 385).2 = 561.(-2) + 385.3$. On a également $11 = 176 - 33.5 = (561 - 385) - (385.3 - 561.2).5 = 561.11 + 385.(-16)$, relation de Bézout entre 561 et 385, puisque $11 = pgcd(561, 385) = pgcd(561, -385)$. On en déduit la relation de Bézout $561.11 + (-385).16 = 11$.

La figure 10 donne une interprétation géométrique du théorème de Bézout basée sur la géométrie affine (voir le cours n° 4).
La fin de cette section est consacrée à établir le lemme de Gauss 2.4.10, qui est "l'instrument" essentiel du lemme d'Euclide 2.5.6, et donc du théorème de Gauss 2.5.7 sur la décomposition des entiers relatifs en facteurs premiers.

**Proposition 2.4.8.** *Si $m, n$ et $p$ sont trois entiers relatifs non nuls, alors :*
*i) $m \wedge n$ est un plus grand diviseur commun de $m$ et $n$ au sens de $|$; autrement dit, pour tout $d \in \mathbb{Z}$ tel que $d | m, n$, on a $d | m \wedge n$*
*ii) On a $|p| \times (m \wedge n) = (p \times m) \wedge (p \times n)$.*

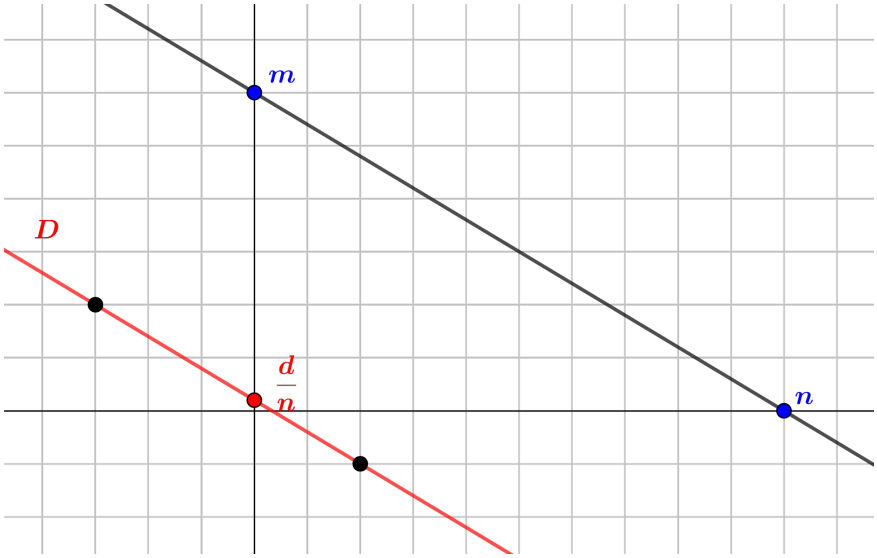



Figure 10: Interprétation géométrique du théorème de Bézout : pour $m, n \in \mathbb{Z}$ non nuls, on reporte $m$ en ordonnée et $n$ en abscisse. La droite $D$ d'équation $mx+ny = d$, où $d = pgcd(m, n)$, est parallèle à la droite joignant les points $(0, m)$ et $(n, 0)$, et les couples $(u, v) \in \mathbb{Z}^2$ tels que $mu + nv = d$ sont les noeuds du plan (points à coordonnées entières) situés sur $D$. Ils fournissent les relations de Bézout entre $m$ et $n$. Ici, on a $m = 6$ et $n = 10$, et les deux points $(-3, 2)$ et $(2, -1)$ conviennent : on a $2 = 6.(-3) + 10.2 = 6.2 + 10.(-1)$.

*Démonstration.* i) Par le théorème de Bézout 2.4.3, il existe $u, v \in \mathbb{Z}$ tels que $m \wedge n = mu + nv$. Supposons que $d \in \mathbb{Z}$ est un diviseur commun de $m$ et $n$ : on a $d|mu, nv$, donc $d|mu + nv = m \wedge n$.
ii) Si $d \in \mathbb{Z}$ et $d|m, n$, alors on a $pd|pm, pn$, d'où $pd|(pm \wedge pn)$ par (i); en particulier, on a $p \times (m \wedge n)|(pm \wedge pn)$. Inversement, comme $p|pm \wedge pn$ puisque $p|pm, pn$, il existe $q \in \mathbb{Z}$ tel que $pq = pm \wedge pn$, donc aussi $pq|pm$ et $pq|pn$ : il existe $u, v \in \mathbb{Z}$ tels que $pm = upq$ et $pn = vpq$, d'où $p(m - uq) = 0$ et $p(n - vq) = 0$, si bien que $m = uq$ et $n = vq$ par intégrité (théorème 2.2.6), et finalement $q|m, n$. Par (i) à nouveau, on a $q|m \wedge n$, d'où $pm \wedge pn = pq|p \times (m \wedge n)$. Par conséquent, on a à la fois $p \times (m \wedge n)|pm \wedge pn$ et $pm \wedge pn|p \times (m \wedge n)$, d'où $p \times (m \wedge n) = pm \wedge pn$ ou $p \times (m \wedge n) = -(pm \wedge pn)$, soit $|p| \times (m \wedge n) = |p \times (m \wedge n)| = (p \times m) \wedge (p \times n)$ (le second membre de l'égalité est toujours positif). □

**Remarque 2.4.9.** Lorsque $m, n, p \in \mathbb{N}$, on peut supprimer les valeurs absolues dans (ii).

**Théorème 2.4.10** (Lemme de Gauss)**.** *Si $m, n$ et $p$ sont des entiers relatifs non nuls, et si $m$ divise $np$ et $m$ et $n$ sont premiers entre eux, alors $m$ divise $p$.*

*Démonstration.* Par la proposition 2.4.8(ii), on a $mp \wedge np = |p| \times (m \wedge n)$ et comme $m \wedge n = 1$, on en déduit que $mp \wedge np = |p|$. Mais $m|np$ par hypothèse, si bien que $m|(mp \wedge np) = |p|$ par la proposition 2.4.8(i), donc $m|p$ également. □

**Remarque 2.4.11.** Ici, le contenu essentiel du théorème a déjà été traité dans la proposition 2.4.8.

### Exercices de la section

*Exercice* 2.4.12. i) Si $m$ et $n$ sont deux entiers relatifs non tous deux nuls, démontrer que le p.g.c.d $m \wedge n$ de $m$ et $n$ est le plus grand entier relatif $d$ tel que $d$ divise à la fois $m$ et $n$, autrement dit que $d|m, n$ et que si $k \in \mathbb{Z}$ et $k|m, n$, alors $k \leq d$.
ii) Trouver une relation de Bézout entre 63 et $-175$.
iii) Montrer que 77 divise 15400 et que 77 et 39 sont premiers entre eux. En déduire que 77 divise 385.

## 2.5 Nombres premiers

### 2.5.1 Puissances des entiers relatifs

Nous avons esquissé une définition des puissances entières des nombres complexes dans le cours n° 1. Puisque nous disposons désormais d'une justification rigoureuse des définitions par récurrence, nous pouvons définir proprement les puissances entières des nombres entiers relatifs, dont nous ferons usage en arithmétique.

**Définition 2.5.1.** Soient $m$ un nombre entier relatif et $n$ un nombre entier naturel. On définit le nombre entier relatif $m$ *(à la) puissance* $n$, noté $m^n$, par récurrence, de la manière suivante :
i) Si $n = 0$, on pose $m^0 = 1$
ii) On pose $m^{n+1} := m^n.m$, en supposant que $m^n$ est défini.

Les amateurs de mathématiques sont souvent gênés par la définition de la puissance zéro, et en particulier de $0^0$ : comment une puissance de 0 peut-elle valoir 1 ?
Sur le plan conceptuel, la puissance $n$-ième d'un nombre quelconque est la formalisation de la multiplication de ce nombre "$n-1$ fois par lui-même". Or, la situation est analogue à ce qu'est la multiplication d'un entier $m$ par un entier naturel $n$, à savoir l'addition de $m$ "$n-1$ fois à lui-même".
En ce qui concerne l'addition, ajouter "0 fois un nombre à lui-même", cela revient à ne rien ajouter, donc ajouter 0, ce qu'on appelle l'élément *neutre* de l'addition. L'élément neutre de la multiplication étant 1, par analogie la multiplication d'un nombre "0 fois par lui-même" revient à ne le multiplier par rien, c'est-à-dire à le multiplier par 1.
Sur le plan strictement mathématique, c'est aussi la seule définition qui permet d'obtenir les propriétés intuitives générales des puissances entières, que nous énonçons ici :

**Proposition 2.5.2.** *Soient $m, n$ des entiers relatifs et $p, q$ des entiers naturels. On a :*
*i)* $(m.n)^p = m^p.n^p$
*ii)* $m^{p+q} = m^p.m^q$
*iii)* $(m^p)^q = m^{p.q}$.

*Démonstration.* i) On procède par récurrence sur $p$. Si $p = 0$, on a $(m.n)^p = (m.n)^0 = 1 = 1.1 = m^0.n^0$. Supposons que la propriété est vraie au rang $p$, c'est-à-dire que $(m.n)^p = m^p.n^p$ : on a alors $(m.n)^{p+1} = (m.n)^p.(m.n)$ (par définition)

$= (m^p).(n^p).m.n$ (par hypothèse de récurrence) $= (m^p).m.(n^p).n = m^{p+1}.n^{p+1}$, ce qui est la propriété au rang $p+1$, et on conclut par récurrence.
ii) On raisonne par récurrence sur $q$, $m$ et $p$ étant donnés. Si $q = 0$, alors $m^{p+q} = m^p = m^p.1 = m^p.m^0 = m^p.m^q$, donc la propriété est vérifiée pour $q = 0$. Supposons qu'elle le soit pour un entier naturel $q$, on a $m^{p+(q+1)} = m^{(p+q)+1} = m^{p+q}.m$ (par définition de la puissance) $= m^p.m^q.m$ (par hypothèse de récurrence) $= m^p.m^{q+1}$ (par définition à nouveau), ce qui est la propriété au rang $q+1$. Les entiers $m$ et $p$ étant choisis de manière arbitraire, la propriété est démontrée par récurrence pour tous $m, p$ et $q$.
iii) Raisonnons à nouveau par récurrence sur $q$ : si $q = 0$, on a $(m^p)^q = (m^p)^0 = 1$ (par définition) $= m^0 = m^{p.0} = m^{p.q}$, et la propriété est vérifiée pour $q = 0$. Supposons qu'elle le soit pour $q$, on a alors $(m^p)^{q+1} = (m^p)^q.m^p$ (par définition) $= m^{p.q}.m^p$ (par hypothèse de récurrence) $= m^{p.q+p}$ (par (ii)) $= m^{p.(q+1)}$, ce qui est la propriété au rang $q+1$, et on conclut par récurrence. □

Les applications d'addition et de multiplication et les puissances entières sont des fonctions "calculables", au sens de la *théorie de la récursivité*, fondement de l'informatique théorique, que nous aborderons plus tard dans le cursus : elles peuvent être décrites par des suites d'instructions ou algorithmes, qui correspondent à des programmes, et ces notions se traduisent rigoureusement sur le plan mathématique. C'est la même définition que nous adopterons pour étendre les puissances à d'autres nombres, et les propriétés analogues sont démontrées de la même manière.
En particulier, dans le Chapitre 3 nous étendrons la définition des puissances entières aux nombres rationnels, et nous pourrons également étendre la définition à des puissances d'un nombre rationnel par un entier *relatif* quelconque.

### 2.5.2 Nombres premiers

Nous avons introduit les nombres entiers naturels *premiers* dans la section 1.5. En étendant cette notion aux nombres entiers relatifs, on n'en change pas essentiellement le contenu, mais on peut invoquer le lemme de Gauss sur les nombres premiers entre eux, pour établir ce qui est peut-être le résultat fondamental de l'arithmétique élémentaire, le théorème de Gauss sur la décomposition en nombres premiers, dont nous donnerons deux versions (les théorèmes 2.5.7 et 2.5.10).

**Définition 2.5.3.** Un nombre entier relatif $p$ est dit *premier*, si $|p|$ est un nombre premier (définition 1.5.1).

**Remarque 2.5.4.** A partir de la définition 1.5.1, on voit immédiatement qu'un entier relatif $p$ est premier si et seulement si ses seuls diviseurs sont $1, -1, p$ et $-p$.

L'étude, à la section précédente, de la primalité relative, permet d'utiliser la "structure" arithmétique de l'ensemble $\mathbb{Z}$ pour avancer plus loin dans la théorie des nombres premiers.

**Lemme 2.5.5.** *Si $n$ est un entier relatif et $p$ un nombre premier, alors soit $p$ divise $n$, soit $p$ et $n$ sont premiers entre eux.*

*Démonstration.* Par définition, le pgcd $n \wedge p$ de $n$ et $p$ divise à la fois $n$ et $p$, donc $n \wedge p = 1$ ou $n \wedge p = |p|$, puisque $p$ est premier. Si $n \wedge p = |p|$, alors $p$ divise $n$ : par contraposée, si $p \nmid n$ alors $n \wedge p = 1$, c'est-à-dire $n$ et $p$ sont premiers entre eux. □

**Lemme 2.5.6** (Euclide)**.** *Soit $p$ un nombre premier. Si $r \in \mathbb{N}$ est un entier supérieur à 2, et si $m_1, \ldots, m_r$ sont $r$ entiers relatifs tels que $p|m_1 \ldots m_r$, alors il existe $i \in \{1, \ldots, r\}$ tel que $p|m_i$.*

*Démonstration.* On procède par récurrence sur $r \geq 2$. Si $r = 2$ et $p|m_1 m_2$, supposons que $p$ ne divise pas $m_1$ : par le lemme 2.5.5, $p$ et $m_1$ sont premiers entiers eux. Par le lemme de Gauss 2.4.10, on a alors $p|m_2$. Supposons que la propriété est vérifiée au rang $r \geq 2$ et que $m_1, \ldots, m_{r+1}$ sont des entiers naturels tels que $p$ divise le produit $m_1 \ldots m_{r+1}$ : par le cas $r = 2$, soit $p|m_1 \ldots m_r$, soit $p|m_{r+1}$. Dans le premier cas, par hypothèse de récurrence il existe $i \in \{1, \ldots, r\}$ tel que $p|m_i$; dans le second cas, on a $p|m_{r+1}$ donc dans les deux cas il existe $i \in \{1, \ldots, r+1\}$ tel que $p|m_i$, ce qui est la propriété au rang $r+1$. Par le principe de récurrence, la propriété est démontrée pour tout $r \geq 2$. □

Le théorème suivant, fondamental, permet de représenter tous les entiers naturels à partir des nombres premiers; nous en donnons une démonstration approfondie.

**Théorème 2.5.7** (Gauss)**.** *Pour tout entier naturel $n \geq 2$, il existe un entier naturel $m \geq 1$ unique et des entiers naturels premiers uniques $p_1 \leq \ldots \leq p_m$ tels que $n = p_1 \ldots p_m$.*

*Démonstration.* Nous commençons par démontrer l'existence de la décomposition, par récurrence sur $n$. Si $n = 2$, comme 2 est premier, pour $m = 1$ et $p_1 = 2$ on a une décomposition (ou alors, on commence avec $n = 0$ et il n'y a rien à démontrer !). Supposons que $n \geq 3$ et que la décomposition existe pour tous les entiers naturels $m < n$ : par le lemme 1.5.6, $n$ possède un facteur premier, soit donc $p$ le plus petit d'entre eux par la proposition 1.4.3. Si $n$ est premier, on a $n = p$ et donc une décomposition, sinon il existe $q \in \mathbb{N}$ non nul tel que $n = pq$ ($q$ est le quotient de la division de $n$ par $p$). Comme $n \neq p$, on a $q \neq 1$, soit $q \geq 2$, et comme $p < n$, on a aussi $q < n$, donc par hypothèse de récurrence appliquée à $q$, il existe un entier naturel $m$ unique et des nombres premiers $q_1, \ldots, q_m$ tels que $q = q_1 \ldots q_m$ et $q_1 \leq \ldots \leq q_m$. Comme $q_i|n$ pour tout $i = 1, \ldots, m$, par définition de $p$ on a $p \leq q_1$, si bien qu'il existe $m+1$ nombres premiers $p, q_1, \ldots, q_m$ tels que $n = pq_1 \ldots q_m$ et $p \leq q_1 \leq \ldots \leq q_m$ : l'existence de la décomposition est démontrée par récurrence sur $n$.
Supposons que $n = p_1 \ldots p_r$ et démontrons l'unicité de la décomposition, dans un deuxième temps, par récurrence sur $r \geq 1$. On suppose qu'il existe $s \in \mathbb{N}$ et $q_1, \ldots, q_s$ tels que $q_1 \leq \ldots \leq q_s$, et $n = q_1 \ldots q_s$, et on montre que $r = s$ et $p_i = q_i$ pour $i = 1, \ldots, r$. Par le lemme d'Euclide 2.5.6, dans tous les cas il existe $i \in \{1, \ldots, s\}$ tel que $p_1|q_i$ et comme $q_i$ est premier et $p_1 \neq 1$, on a $p_1 = q_i$; par définition de $q_1$, on a alors $q_1 \leq p_1$. En raisonnant de manière symétrique (en échangeant les rôles de $p_1$ et $q_1$), on a également $p_1 \leq q_1$, d'où $p_1 = q_1$. Supposons que $n = p_1$ : dans ce cas, on a aussi $n = q_1$, donc $q_2 \ldots q_s = 1$, ce qui n'est possible que si $s = 1$ (raisonner par l'absurde). La propriété est donc démontrée au rang $r = 1$, supposons qu'elle le

soit au rang $r-1$, pour $r>2$ : on peut écrire $n=p_1m$, où $m=p_2\dots p_r=q_2\dots q_s$. Comme $p_2\leq\dots\leq p_r$ et $q_2\leq\dots\leq q_s$, par hypothèse de récurrence appliquée à $m$, on a $r-1=s-1$, soit $r=s$, et $p_i=q_i$ pour $i=2,\dots,r$, d'où finalement $p_i=q_i$ pour $i=1,\dots,r$, ce qui est la propriété au rang $r$, et le théorème est démontré par récurrence. □

**Remarque 2.5.8.** Cette démonstration n'est pas si simple, et elle imbrique plusieurs types de raisonnement, ce qui est formateur; l'essentiel est d'en comprendre le principe en première lecture.

Nous allons affiner l'énoncé du théorème de Gauss 2.5.7 : celui-ci donne une décomposition dans laquelle certains facteurs premiers peuvent apparaître "plusieurs fois", puisque la condition est donnée par des inégalités larges. Il est possible d'être plus précis, en ordonnant les facteurs premiers *distincts* de manière stricte; il faut alors compter le "nombre de fois que chaque facteur apparaît", sous la forme de puissances de chacun de ces facteurs.

**Lemme 2.5.9.** *Si $n\neq 0$ est un entier naturel non nul et $d\geq 2$, il existe un nombre entier $r$ maximal tel que $d^r|n$.*

*Démonstration.* Montrons d'abord qu'il existe $r\in\mathbb{N}$ tel que $d^r|n$ : on a $d^0=1$, et $1|n$, donc un tel $r$ existe; notons $D$ l'ensemble des puissances de $d$ qui divisent $n$, autrement dit $D=\{m\in\mathbb{N} : \exists r\in\mathbb{N},\ (m=d^r)\wedge(m|n)\}$. Comme $n>0$, on sait également que pour tout $m$ tel que $m|n$, on a $m\leq n$ (exercice 1.3.17(v)), si bien que l'ensemble des diviseurs de $n$, soit $E=\{m\in\mathbb{N} : m|n\}$, est inclus dans l'ensemble $[[0,n]]$. En particulier, l'ensemble $D$ est fini comme sous-ensemble de l'ensemble fini $E$ (cours n° 3, Chapitre 3); il possède donc un plus grand élément par le lemme 1.4.3, qui est de la forme $m=d^r$. Par définition de $m$, on a alors $d^r|n$; comme $d\geq 2$, on a aussi $d^r<d^{r+1}$, d'où $d^{r+1}\nmid n$. Par conséquent, $r$ est l'entier maximal cherché. □

**Théorème 2.5.10.** *Pour tout entier naturel $n\geq 2$, il existe un entier naturel $r\geq 1$ unique, des nombres premiers uniques $p_1<\dots<p_r$ et des nombres entiers uniques $a_1,\dots,a_r\geq 1$ tels que $n=p_1^{a_1}\dots p_r^{a_r}$.*

*Démonstration.* On procède de manière analogue à la démonstration du théorème 2.5.7. Commençons par démontrer l'existence de la décomposition, par récurrence sur $n$. Si $n=2$, comme 2 est premier, pour $r=1$, $p_1=2$ et $a_1=1$ on a une décomposition. Supposons que $n\geq 3$ et que la décomposition existe pour tous les entiers naturels $m<n$ : par le lemme 1.5.6 et la proposition 1.4.3, soit alors $p$ le plus petit facteur premier de $n$. Si $n$ est premier, on a $n=p$ et donc une décomposition, sinon il existe $q\in\mathbb{N}$ tel que $n=pq$ et par hypothèse de récurrence appliquée à $q\geq 2$ il existe un entier naturel $r$, des nombres premiers $q_1,\dots,q_r$ et des entiers $a_1,\dots,a_r\geq 1$ tels que $q=q_1^{a_1}\dots q_r^{a_r}$ et $q_1<\dots<q_r$. Comme alors $q_i|n$ pour tout $i=1,\dots,r$, par définition de $p$ on a $p\leq q_1$, et on distingue deux cas : soit $p=q_1$, et alors on a $n=q_1^{a_1+1}q_2^{a_2}\dots q_r^{a_r}$, ce qui est une décomposition de la forme voulue, soit $p<q_1$, et alors on a $n=pq_1^{a_1}\dots q_r^{a_r}$, ce qui est aussi une décomposition de la forme voulue : l'existence est démontrée par récurrence sur $n$. Supposons que $n=p_1^{a_1}\dots p_r^{a_r}$ avec $p_1<\dots<p_r$ et $a_1,\dots a_r\geq 1$ et démontrons l'unicité de la décomposition, dans un deuxième temps, par récurrence sur $r\geq 1$. Le cas $r=1$ est

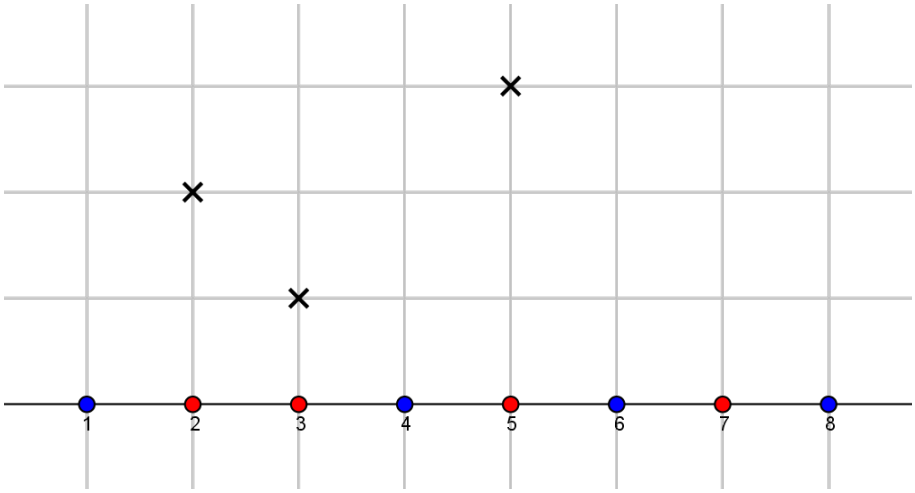



Figure 11: A partir de la décomposition du théorème de Gauss, tout entier naturel non nul peut se représenter de manière géométrique à partir de ses facteurs premiers et de leurs "exposants" dans la décomposition (et cette représentation permet de décrire la multiplication dans $\mathbb{N}^* = \mathbb{N} - \{0\}$ à partir de l'addition dans $\mathbb{N}$). Ici, on a représenté la décomposition de l'entier $1500 = 2^2.3^1.5^3$.

laissé à l'étudiant(e) et on suppose que $r > 2$ et que la propriété est vérifiée au rang $r-1$. Admettons qu'il existe $s \in \mathbb{N}$, $q_1 < \ldots < q_s$ premiers et $b_1, \ldots, b_s \geq 1$ tels que $n = q_1^{b_1} \ldots q_s^{b_s}$, et montrons que $r = s$, $p_i = q_i$ et $a_i = b_i$ pour $i = 1, \ldots, r$. Par le lemme d'Euclide 2.5.6, dans tous les cas il existe $i \in \{1, \ldots, s\}$ tel que $p_1 | q_i$, et comme $q_i$ est premier et $p_1 \neq 1$, on a $p_1 = q_i$; par définition de $q_1$, on a alors $q_1 \leq p_1$ et en raisonnant de manière symétrique on en déduit que $p_1 = q_1$. Supposons que $a_1 \neq b_1$, par exemple $a_1 < b_1$ : en simplifiant l'égalité $p_1^{a_1} \ldots p_r^{a_r} = q_1^{b_1} \ldots q_s^{b_s}$ par $p^{a_1}$ (par 1.2.7 ou 2.2.6), on obtient $p_2^{a_2} \ldots p_r^{a_s} = q_1^{b_1 - a_1} q_2^{b_2} \ldots q_s^{b_s}$, donc $q_1 = p_1$ divise l'un des $p_i$ par le lemme d'Euclide à nouveau, ce qui est exclu car $p_i$ est premier et différent de $p_1$ pour tout $i = 2, \ldots, r$. On en conclut en raisonnant de manière symétrique que $a_1 = b_1$, si bien que $m := p_2^{a_2} \ldots p_r^{a_r} = q_2^{b_2} \ldots q_r^{b_r}$ : par hypothèse de récurrence appliquée à $m$, on a $r - 1 = s - 1$, soit $r = s$, $p_i = q_i$ pour $i = 2, \ldots, r$, et $a_i = b_i$ pour $i = 2, \ldots, r$, et on a donc montré la propriété au rang $r$, et le théorème est démontré par récurrence. □

La figure 11 propose une représentation graphique de la décomposition d'un nombre entier naturel en puissances de nombres premiers.
Les théorèmes 2.5.7 et 2.5.10 sont énoncés en termes de nombres entiers naturels. Il est assez simple, mais un peu complexe à écrire, de les généraliser sous une forme valable pour tous les nombres entiers relatifs. Nous réserverons cette approche à une étude plus générale, en notant simplement ici qu'une décomposition d'un nombre entier relatif quelconque $n$ non nul est obtenue facilement à partir de la décomposition de $|n|$ : si $|n| = p_1^{a_1} \ldots p_r^{a_r}$, on obtient $n = -|n| = -p_1^{a_1} \ldots p_n^{a_n}$, où les $p_i$ sont des entiers naturels premiers. Si nous nous limitons ici aux entiers naturels, il ne faut pas oublier que nous avons bâti la décomposition sur la théorie des entiers relatifs premiers entre eux, car nous en avions besoin pour le lemme d'Euclide 2.5.6.

### Exercices de la section

*Exercice* 2.5.11. i) Démontrer que les nombres $-5, -7, 11, -13, 17$ et $-19$ sont premiers (utiliser la section 1.5).
ii) Décomposer 2520 et $-1617$ en nombres premiers. Ces deux nombres sont-ils premiers entre eux ?

## 2.6 Nombres primaires et plus petit commun multiple

### 2.6.1 Nombres primaires

**Définition 2.6.1.** Un nombre entier naturel $q$ est dit *primaire* si c'est une puissance d'un nombre premier, autrement dit s'il existe un entier naturel premier $p$ et un entier naturel $r \geq 1$ tels que $q = p^r$.

**Exemple 2.6.2.** Les nombres $4 = 2^2$, $9 = 3^2$ et $125 = 5^3$ sont des nombres primaires.

**Lemme 2.6.3.** *Si $p$ est un entier naturel premier et $r \geq 1$, les diviseurs positifs de $p^r$ sont $1, p, \ldots, p^r$, c'est-à-dire $\{p^k : k = 0, \ldots, r\}$.*

*Démonstration.* Supposons que $d \in \mathbb{N}$ et que $d|p^r$ : on procède par récurrence sur $r \geq 1$. Si $r = 1$, on a $d|p$, et comme $p$ est premier on a $d = 1$ ou $d = p$ et la propriété est vérifiée. Supposons que $r \geq 1$ et que $d|p^{r+1}$ : si $d \neq 1$, comme tout entier naturel possède un facteur premier par le lemme 1.5.6, il existe un entier naturel premier $q$ tel que $q|d$, donc aussi $q|p^{r+1}$. Par le lemme d'Euclide 2.5.6, on a alors $q|p$, si bien que $q = p$, donc finalement $p|d$. On peut donc écrire $p^{r+1} = d.m$ et $d = p.n$ pour $m, n \in \mathbb{N}$, soit $p^{r+1} = d.m = p.m.n$ et par la proposition 1.2.7 on en déduit que $p^r = m.n$. Par hypothèse de récurrence, on a $n \in \{1, \ldots, p^r\}$, si bien que $d = p.n \in \{p, p^2, \ldots, p^{r+1}\}$, et on conclut par récurrence. □

**Corollaire 2.6.4.** *Si $n$ est un entier relatif non nul et différent de 1 et $-1$, il existe un entier naturel $r \geq 1$ unique et des nombres primaires $q_1, \ldots, q_r$ deux-à-deux premiers entre eux et uniques tels que $n = q_1 \ldots q_r$ ou $n = -q_1 \ldots q_r$.*

*Démonstration.* Par le théorème 2.5.10, il existe $r \geq 1$, des entiers naturels premiers $p_1 < \ldots < p_r$ et des entiers naturels $a_1, \ldots, a_r \geq 1$ tels que $|n| = p_1^{a_1} \ldots p_r^{a_r}$ : en posant $q_i = p_i^{a_i}$ pour tout $i = 1, \ldots, r$, on peut donc écrire $|n| = q_1 \ldots q_r$. Les $q_i$ sont primaires, et si $i \neq j$, on a $p_i \neq p_j$, donc $q_i$ et $q_j$ sont premiers entre eux (en effet, par le lemme 2.6.3 un facteur commun à $q_i$ et $q_j$ est de la forme $p_i^{c_i}$, et si $c_i \neq 0$ on a $p_i|q_j$, soit $p_i = q_j$ par le lemme d'Euclide 2.5.6). En ce qui concerne l'unicité, supposons que $|n| = q_1 \ldots q_r = q'_1 \ldots q'_s$, avec les $q_i$ et les $q'_j$ primaires et $r, s \geq 1$. Ecrivons $q_i = p_i^{a_i}$ et $q'_j = (p'_j)^{b_j}$ avec $p_i$ et $p'_j$ premiers pour $i = 1, \ldots, r$ et $j = 1, \ldots, s$ : comme les $q_i$ sont deux-à-deux premiers entre eux, les $p_i$ sont distincts et quitte à les renuméroter on peut supposer que $p_1 < \ldots < p_r$; de même, les $p'_j$ sont distincts et on peut supposer que $p'_1 < \ldots < p'_s$. Par le théorème 2.5.10, on en déduit que $r = s$, $p_i = p'_i$ et $a_i = b_i$ pour $i = 1, \ldots, r$. Finalement, on a $q_i = q'_i$ pour tout $i = 1, \ldots, r$, et l'unicité est démontrée. □

**Remarque 2.6.5.** i) On a vraiment besoin de la version "forte" de la décomposition en nombres premiers pour cette décomposition unique en nombres primaires : le théorème 2.5.7 ne suffit pas.
ii) La donnée de $p_1, \dots, p_r$ correspondant à un $r$-uplet, c'est-à-dire une application de $[[1, r]]$ dans $\mathbb{N}$ (en fait dans l'ensemble des nombres premiers), ne tient pas compte de leur ordre lorsqu'elle est associée comme ici à une décomposition en nombres primaires $q_1, \dots, q_r$. La "renumérotation" dont il est question revient donc à décrire un autre $r$-uplet, dont l'image est la même, mais qui prend en compte l'ordre de ces nombres premiers. La description de ce procédé est laissée en exercice. Noter que l'unicité de l'énoncé est en ce sens quelque peu "impropre", car changer la numérotation des $q_i$ donne une autre décomposition; la décomposition est donc unique "à permutation près" des nombres $q_1, \dots, q_r$.

Soient $n$ un entier relatif non nul et $p$ un entier naturel premier. Par le lemme 2.5.9, il existe un entier naturel $r$ maximal tel que $p^r | n$.

**Définition 2.6.6.** Si $n$ est un entier relatif non nul et $p$ un nombre premier, on appelle *exposant de $p$ dans $n$* l'entier naturel $r$ maximal tel que $p^r | n$.

**Proposition 2.6.7.** *Si $p \in \mathbb{N}$ est un nombre premier et $m, n \in \mathbb{Z}$ sont deux entiers relatifs non nuls, alors l'exposant de $p$ dans $m.n$ est la somme de l'exposant de $p$ dans $m$ et de l'exposant de $p$ dans $n$.*

*Démonstration.* Soient $r$ et $s$ les exposants respectifs de $p$ dans $m$ et $n$, de sorte qu'on peut écrire $m = p^r.a$ et $n = p^s.b$ avec $p \nmid a$ et $p \nmid b$. On a alors $m.n = (p^r.a).(p^s.b) = p^{r+s}.ab$, donc l'exposant $u$ de $p$ dans $m.n$ est supérieur à $r + s$. Mais supposons par l'absurde que $p^{r+s+1} | m.n$ : on peut alors écrire $m.n = p^{r+s+1}.c = p^{r+s}.ab$; en simplifiant par $p^{r+s}$ par la proposition 2.2.6, on obtient $pc = ab$, et par le lemme d'Euclide 2.5.6 on a $p|a$ ou $p|b$, ce qui est impossible. Par *reductio ad absurdum*, on en déduit que $r + s$ est l'exposant de $p$ dans $m.n$. □

La proposition suivante paraît évidente, mais il faut la démontrer proprement.

**Proposition 2.6.8.** *Si $n$ est un entier naturel non nul et $n = p_1^{a_1} \dots p_r^{a_r}$ est sa décomposition en entiers naturels premiers (théorème 2.5.10), alors pour tout $i = 1, \dots, r$ l'exposant de $p_i$ dans $n$ est $a_i$.*

*Démonstration.* Par définition, pour tout $i$ on a $p_i^{a_i} | n$, donc l'exposant $e_i$ de $p_i$ dans $n$ est supérieur à $a_i$. Supposons par l'absurde que $e_i > a_i$ : on peut alors écrire $n = p_i^{e_i} m = p_1^{a_1} \dots p_r^{a_r}$, donc en simplifiant par la proposition 1.2.7 on obtient $p_i^{e_i - a_i} m = p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \dots p_r^{a_r}$. Par le lemme d'Euclide 2.5.6, $p_i$ divise alors l'un des $p_j$ pour $j \neq i$, ce qui est impossible. Par *reductio ad absurdum*, on en déduit que $e_i \leq a_i$, et donc finalement que $e_i = a_i$. □

**Proposition 2.6.9.** *Soient $m, n \in \mathbb{Z}$ non nuls. Alors, on a $m|n$ si et seulement si pour tout nombre premier $p$, l'exposant de $p$ dans $m$ est inférieur à l'exposant de $p$ dans $n$.*

*Démonstration.* Quitte à prendre les valeurs absolues (puisque le signe ne change pas les propriétés de divisibilité) il suffit de travailler avec $m, n \in \mathbb{N}$. Ecrivons la décomposition de $n$ en entiers naturels premiers : on a $n = p_1^{a_1} \dots p_r^{a_r}$, avec $p_1 < \dots < p_r$ et $a_i \geq 1$ pour tout $i$. De même, écrivons la décomposition de $m$ : on a $m = q_1^{b_1} \dots q_s^{b_s}$. Supposons que $m|n$ : pour tout $j = 1, \dots, s$, on a $q_j|n$ donc par le lemme d'Euclide 2.5.6 il existe $i$ tel que $q_j = p_i$; autrement dit, les facteurs premiers $q_j$ de $m$ sont des facteurs premiers de $n$. On peut donc réécrire $m = p_1^{b_1} \dots p_r^{b_r}$, avec $b_i \in \mathbb{N}$ pour tout $i$ (certains étant éventuellement nuls). Supposons que $b_i > a_i$ : l'exposant $e_i$ de $p_i$ dans $n$ est alors $> a_i$, ce qui est impossible par la proposition 2.6.8; on en déduit que $b_i \leq a_i$ pour tout $i$. Plus généralement, comme tout facteur premier de $m$ est l'un des $p_i$, on en déduit que l'exposant de tout nombre premier $p$ dans $m$ est inférieur à son exposant dans $n$. Inversement, avec les mêmes notations si l'exposant de tout nombre premier $p$ dans $m$ est inférieur à son exposant dans $n$, alors seuls les nombres premiers $p_1, \dots, p_n$ peuvent être des facteurs premiers de $m$, c'est-à-dire y avoir un exposant strictement positif, si bien qu'on peut écrire $m = p_1^{b_1} \dots p_r^{b_r}$ avec $b_i \leq a_i$ pour tout $i$. On a alors $n = m.k$ avec $k = p_1^{a_1 - b_1} \dots p_r^{a_r - b_r}$, si bien que $m|n$. □

**Corollaire 2.6.10.** *Soient $m$ et $n$ deux entiers relatifs non nuls et $p_1 < \dots < p_r$ les entiers naturels premiers apparaissant dans la décomposition de $m$ et $n$ en facteurs premiers, de sorte que $|m| = p_1^{a_1} \dots p_r^{a_r}$ et $|n| = p_1^{b_1} \dots p_r^{b_r}$, avec $a_i, b_i \geq 0$ pour tout $i$. Alors, le p.g.c.d de $m$ et $n$ est l'entier naturel $p_1^{\min(a_1, b_1)} \dots p_r^{\min(a_r, b_r)}$.*

*Démonstration.* Par la proposition 2.6.9, il est clair que l'entier naturel donné par l'expression de l'énoncé divise à la fois $m$ et $n$, donc il divise $m \wedge n$. Inversement, comme $m \wedge n$ divise à la fois $m$ et $n$, par la même proposition l'exposant de $p_i$ dans $m \wedge n$ est inférieur à la fois à $a_i$ et $b_i$, donc à $\min(a_i, b_i)$ pour $i = 1, \dots, r$, tandis que l'exposant d'un nombre premier $p$ différent de tous les $p_i$ y est nul. Par la proposition 2.6.9 à nouveau, $m \wedge n$ divise l'entier donné par l'expression de l'énoncé, ils sont donc égaux. □

### 2.6.2 Plus petit commun multiple

La proposition 2.4.8 caractérise le p.g.c.d de deux entiers relatifs non nuls $m$ et $n$ comme le "plus grand" diviseur commun de $m$ et $n$, au sens de la relation de divisibilité $|$.
La notion duale, ayant trait aux multiples communs de $m$ et $n$, est celle de "plus petit commun diviseur", au sens de la divisibilité. Cette notion est introduire grâce à la propriété suivante :

**Proposition 2.6.11.** *Si $m$ et $n$ deux sont deux entiers relatifs non nuls, alors le produit $mn$ est divisible par $m \wedge n$, et le quotient $k$ de $mn$ par $m \wedge n$ est un multiple commun de $m$ et $n$, et divise tout multiple commun de $m$ et $n$. De plus, le nombre $|k|$ est l'unique entier naturel possédant cette propriété.*

*Démonstration.* Notons $d = m \wedge n$ : par définition du p.g.c.d, il existe des entiers relatifs $m'$ et $n'$ tels que $m = d.m'$ et $n = d.n'$. Comme par définition, on a $m.n = k.d$, on en déduit les égalités $m.n = d.m'.n = d.k$ et $m.n = d.n'.m = d.k$,

et comme $d \neq 0$, par la proposition 2.2.6 on a $m'.n = k$ et $n'.m = k$, si bien que $k$ est un multiple de $m$ et de $n$. Soit $l \in \mathbb{Z}$ un multiple quelconque de $m$ et $n$ : il existe $a, b \in \mathbb{Z}$ tels que $l = a.m$ et $l = b.n$, d'où $am = bn$, soit $a.d.m' = b.d.n'$ et à nouveau $am' = bn'$ par intégrité. Or, par la proposition 2.4.8(ii), on a $d.(m' \wedge n') = (d.m') \wedge (d.n') = m \wedge n = d$, donc par intégrité encore, on a $m' \wedge n' = 1$, c'est-à-dire $m'$ et $n'$ sont premiers entre eux. Par le lemme de Gauss 2.4.10, on en déduit que $m'$ divise $b$, donc $k = m'n$ divise $bn = l$, et la propriété de $k$ est démontrée. Par ailleurs, il est clair que $|k|$ possède aussi cette propriété. Supposons alors que $k'$ est un entier naturel possédant la même propriété : on a alors $k|k'$ (puisque $k'$ est un multiple comme de $m$ et $n$) et $k'|k$ (pour la même raison). Comme $|k|$ et $k'$ sont positifs, on a donc $|k| = k'$. □

**Remarque 2.6.12.** i) Au cours de la démonstration, nous avons établi que si $m$ et $n$ sont des entiers relatifs non nuls, alors $m/(m \wedge n)$ et $n/(m \wedge n)$ sont premiers entre eux.
ii) L'étudiant(e) gêné(e) en première lecture par l'utilisation des valeurs absolues, peut commencer par étudier cette proposition et sa démonstration en travaillant avec $m, n \in \mathbb{N}$ et en supprimant les valeurs absolues.

**Définition 2.6.13.** Le *plus petit commun multiple (p.p.c.m)* de deux entiers relatifs $m$ et $n$ non nuls est l'entier naturel $|mn|/(m \wedge n)$, noté $ppcm(m, n)$ ou $m \vee n$.

La notion de plus grand commun diviseur s'interprète en termes de la relation d'ordre large $\leq$ sur les entiers naturels au niveau des exposants des facteurs premiers, dans le corollaire 2.6.10 : on trouve le p.g.c.d de $m$ et $n$ en choisissant pour chaque nombre premier $p$ le plus grand exposant inférieur à la fois à l'exposant de $p$ dans $m$ et dans $n$, c'est-à-dire le minimum, introduit dans la section 1.3.11.
La notion duale du minimum est celle de maximum, ce qui permet d'interpréter la notion de plus petit commun multiple en termes de *maximum* des exposants dans les décompositions en nombres premiers.

**Lemme 2.6.14.** *Soient $a$ et $b$ deux entiers relatifs, alors on a* $a + b = \min\{a, b\} + \max\{a, b\}$.

*Démonstration.* Distinguons deux cas. Si $a \leq b$, alors $\min\{a, b\} = a$ et $\max\{a, b\} = b$, donc le membre de droite de l'équation est $a + b$, et l'égalité est vérifiée. Si $b < a$, alors $\min\{a, b\} = b$ et $\max\{a, b\} = a$, et le membre de droite est $b + a$, et l'égalité est encore vérifiée par commutativité de l'addition. □

**Proposition 2.6.15.** *Si $m$ et $n$ sont deux entiers relatifs non nuls et $p_1 < \ldots < p_r$ sont les entiers naturels premiers apparaissant dans la décomposition de $m$ et $n$ en facteurs premiers, avec $|m| = p_1^{a_1} \ldots p_r^{a_r}$ et $|n| = p_1^{b_1} \ldots p_r^{b_r}$ pour $a_i, b_i \geq 0$, alors le p.p.c.m de $m$ et $n$ est l'entier naturel $p_1^{\max(a_1,b_1)} \ldots p_r^{\max(a_r,b_r)}$.*

*Démonstration.* Notons $k$ le p.p.c.m $m \vee n = |mn|/(m \wedge n)$ de $m$ et $n$, de sorte que $|mn| = k.(m \wedge n)$. On a $|mn| = |m|.|n| = (p_1^{a_1} \ldots p_r^{a_r}).(p_1^{b_1} \ldots p_r^{b_r}) = p_1^{a_1+b_1} \ldots p_r^{a_r+b_r}$. Comme $k \mid |mn|$, tout facteur premier $p$ de $k$ est un facteur premier de $|mn|$, c'est donc l'un des nombres premiers $p_i$ par le lemme d'Euclide 2.5.6 : il s'ensuit qu'on peut écrire $k$ sous la forme $k = p_1^{e_1} \ldots p_r^{e_r}$, avec $e_i \geq 0$ pour tout $i$. Par le corollaire

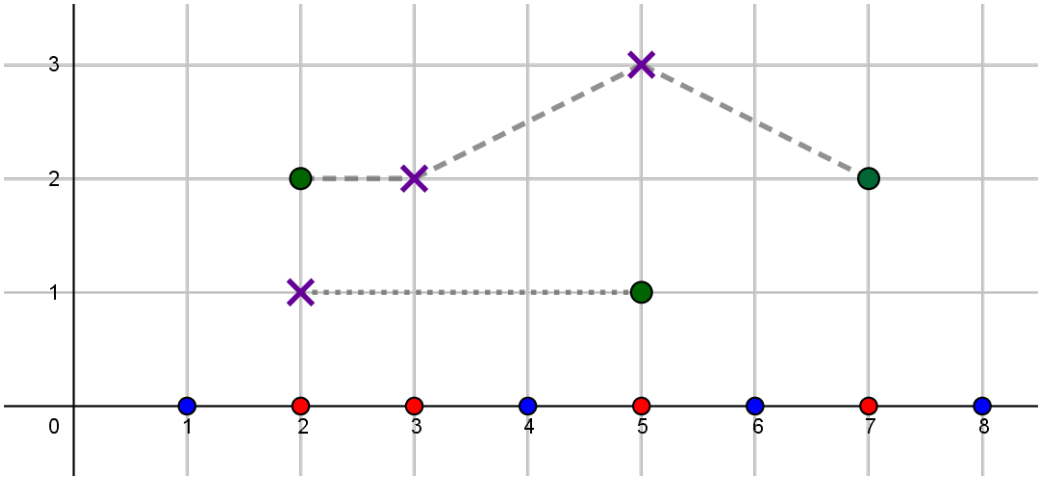



Figure 12: L'entier naturel représenté par les croix (en violet) est $2.3^2.5^3 = 2250$ et l'entier naturel représenté par les points (en vert) est $2^2.5.7^2 = 980$. On obtient leur p.g.c.d, $2.5 = 10$, en choisissant les plus petits exposants des facteurs communs aux deux (chemin du bas), et leur p.p.c.m, $2^2.3^2.5^3.7^2 = 220500$, en choisissant les plus grands exposants de tous les facteurs présents (chemin du haut).

2.6.10, on a donc $p_1^{a_1+b_1} \dots p_r^{a_r+b_r} = |mn| = k(m \wedge n) = p_1^{e_1+\min(a_1,b_1)} \dots p_r^{e_r+\min(a_r,b_r)}$. Par unicité de la décomposition en nombres premiers de cet entier naturel (théorème 2.5.10), on en déduit pour tout $i = 1, \dots, r$ que $a_i + b_i = e_i + \min(a_i, b_i)$, ou encore que $e_i = a_i + b_i - \min(a_i, b_i) = \max(a_i, b_i)$ par le lemme 2.6.14 : c'est ce qu'il fallait démontrer. □

La figure 12 donne une interprétation géométrique du p.g.c.d et du p.p.c.m de deux entiers relatifs, à partir de leur décomposition en nombres premiers.

### Exercices de la section

*Exercice* 2.6.16. i) Décomposer 2520 et 6750 en nombres primaires, et en déduire leur p.g.c.d et leur p.p.c.m.
ii) Trouver le p.g.c.d de $-819$ et 5775 et en déduire leur p.p.c.m.

## 2.7 Arithmétique modulaire

L'arithmétique modulaire est l'étude des propriétés arithmétiques (associées à la multiplication) des entiers relatifs *modulo* un entier naturel non nul $b$. Cela signifie que l'on considère (l'addition et) la multiplication d'entiers relatifs $m$ et $n$ du point de vue du *reste* de la division euclidienne de $m.n$ par $b$. L'addition et la multiplication des entiers modulo $b$ possède en effet des propriétés tout-à-fait analogues à celles des entiers relatifs.
Cette partie de l'arithmétique, source de nombreuses applications notamment en cryptographie, est fondamentale, d'abord en ce qu'elle permet de donner des critères de divisibilité, ensuite en ce qu'elle permet d'énoncer des théorèmes d'arithmétique

dans un cadre naturel qui trouvera son lieu au semestre II dans la théorie des "structures algébriques", en l'espèce la théorie des *anneaux*.
L'arithmétique ou théorie des nombres ne s'intéresse en effet pas seulement aux ensembles classiques de nombres $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, mais aussi à des ensembles plus exotiques apparaissant notamment avec l'arithmétique modulaire, et dont la connaissance permet une compréhension approfondie de ces ensembles naturels.

### 2.7.1 Les relations de congruence sur $\mathbb{Z}$

La relation fondamentale entre entiers relatifs, qui permet de fonder l'arithmétique modulaire, est celle de *congruence*, laquelle formalise la situation où deux entiers relatifs $m$ et $n$ **ont le même reste** dans la division euclidienne par un entier naturel non nul $b$ donné.
Effectuons en effet la division euclidienne de $m$ et $n$ par $b$ : il existe par le théorème 2.2.14 des entiers relatifs $q$ et $q'$ uniques, et des entiers naturels $r, r' \in \{0, \dots, b-1\}$ uniques, tels que $m = b.q + r$ et $n = b.q' + r'$. On peut donc écrire $m - n = b.(q-q')+(r-r')$. Or, supposons que $m$ et $n$ ont le même reste, c'est-à-dire que $r = r'$ : on a alors $m-n = b.(q-q')$, donc $b$ *divise* $m-n$. Mais la réciproque est également vraie : si $b$ divise $m-n$, il existe $d \in \mathbb{Z}$ tel que $m - n = b.d = b.(q-q') + (r-r')$, d'où $b.(d-q+q') = r-r'$. Or, on a $1-b \leq -r' \leq 0$ (puisque $r' \in [[0, b-1]]$), d'où $1-b \leq r-r' \leq b-1$, c'est-à-dire $|r-r'| < b$, si bien que $|r-r'| = 0$ (puisque $b$ divise $|r-r'|$), et donc $r = r'$. Nous avons donc démontré la proposition suivante :

**Proposition 2.7.1.** *Si $m$ et $n$ sont deux entiers relatifs et $b > 0$ est un entier naturel, alors on a $b|(m-n)$ si et seulement si $m$ et $n$ ont le même reste dans la division euclidienne par $b$.*

A partir de cette propriété, nous pouvons poser la définition suivante :

**Définition 2.7.2.** Si $b$ est un entier naturel non nul, on dit que deux entiers relatifs $m$ et $n$ sont *congrus modulo* $b$ (ou que $m$ *est congru à* $n$ *modulo* $b$), si $b$ divise la différence $m-n$. On note $m \equiv n\ [b]$ la relation binaire "$m$ est congru à $n$ modulo $b$" sur l'ensemble des entiers relatifs.

**Exemple 2.7.3.** i) Deux nombres pairs $n$ et $m$ sont toujours congrus modulo 2. En effet, on peut écrire $n = 2k$ et $m = 2l$ pour $k, l \in \mathbb{Z}$, d'où $n-m = 2k-2l = 2(l-k)$. De même, deux nombres *impairs* $n$ et $m$ sont toujours congrus modulo 2 : on peut écrire $n = 2k+1$ et $m = 2l+1$ avec $k, l \in \mathbb{Z}$, d'où $n-m = (2k+1)-(2l+1) = 2(k-l)$ à nouveau.
ii) En général si $b > 0$ et $n$ est un entier relatif quelconque, $n$ est congru modulo $b$ à l'un des nombres $0, 1, \dots, b-1$, puisque $n$ est congru à son reste dans la division euclidienne

Deux entiers relatifs $m$ et $n$ sont donc congrus modulo $b > 0$ lorsque leur différence est un multiple de $b$. Cette relation de congruence modulo $b$ (qui est une relation binaire sur l'ensemble $\mathbb{Z}$) est ce que nous définirons de manière abstraite au semestre II comme une "relation d'équivalence", concept qui servira à la construction des ensembles $\mathbb{Z}$, $\mathbb{Q}$, et $\mathbb{R}$ à partir de l'axiomatique de Peano et des principes de la théorie naïve des ensembles. La congruence possède les propriétés suivantes :

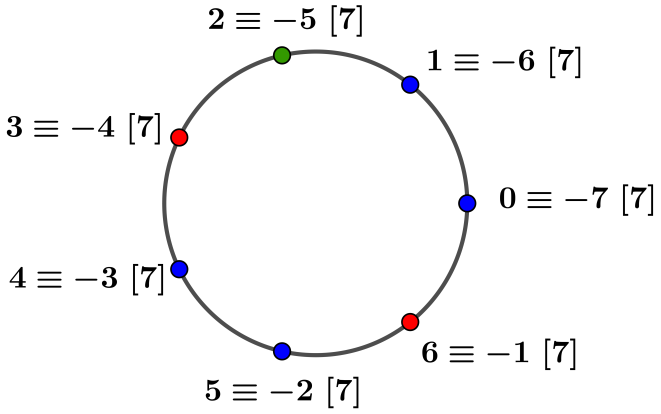



Figure 13: Représentation des relations de congruence modulo 7 des nombres $-7, -6, \ldots, -1$ aux restes possibles dans la division euclidienne par 7, et de l'addition "modulo 7". L'addition se fait directement en "tournant" à partir du premier terme dans le sens anti-horaire; par exemple, l'addition de 3 et de 6 s'obtient en tournant de 6 septièmes de tours à gauche depuis 3 : on obtient $3+6 = 9 \equiv 2\ [7]$. Alternativement, on peut ajouter $-1$ en soustrayant 1 à 3 en tournant dans l'autre sens d'un septième de tour, pour obtenir le même résultat.

**Proposition 2.7.4.** *Soient $b$ un entier naturel non nul et $m, n, k$ trois nombres entiers relatifs.*
*i) Le nombre $n$ est congru à lui-même modulo $b$.*
*ii) Si $m$ est congru à $n$ modulo $b$, alors $n$ est congru $m$ modulo $b$.*
*iii) Si $m \equiv n\ [b]$ et $n \equiv k\ [b]$, alors $m \equiv k\ [b]$.*

*Démonstration.* i) On a $b \mid 0 = n - n$.
ii) Si $m \equiv n\ [b]$, c'est par définition que $b \mid m - n$, donc il existe $d \in \mathbb{Z}$ tel que $m - n = d.b$, d'où $n - m = -(m - n) = (-d).b$, et $b \mid n - m$, c'est-à-dire $n \equiv m\ [b]$.
iii) Si $m \equiv n\ [b]$ et $n \equiv k\ [b]$, alors il existe deux entiers relatifs $d, d'$ tels que $m - n = d.b$ et $n - k = d'.b$, d'où $m - k = (m - n) + (n - k) = d.b + d'.b = (d + d').b$, et $b \mid m - k$, c'est-à-dire $m \equiv k\ [b]$. □

La figure 13 propose une représentation des relations de congruence et de l'addition de quelques nombres entiers modulo 7.
Au niveau élémentaire où nous nous plaçons ici, l'intérêt des relations de congruence réside principalement en ce que les opérations d'addition, de soustraction et de multiplication des entiers relatifs sont "compatibles" à ces relations, dans le sens suivant :

**Proposition 2.7.5.** *Soient $m, m', n$ et $n'$ des entiers relatifs, $b$ un entier naturel non nul tels que $m \equiv m'\ [b]$ et $n \equiv n'\ [b]$, et $k$ un entier naturel.*
*i) On a $m + n \equiv m' + n'\ [b]$*
*ii) On a $m.n \equiv m'.n'\ [b]$*
*iii) On a $m^k \equiv (m')^k\ [b]$.*

*Démonstration.* Par définition, il existe des entiers $d, d'$ tels que $m - m' = d.b$ et $n - n' = d'.b$.

i) On a $(m+n)-(m'+n') = (m-m')+(n-n') = d.b - d'.b = (d-d').b$, ce qui montre que $m+n \equiv m'+n'$ $[b]$.
ii) On a $m.n - m'.n' = m.n - m.n' + m.n' - m'.n' = m.(n-n') - (m'-m).n' = md'b - dbn' = (md' - dn').b$, ce qui montre que $m.n \equiv m'.n'$ $[b]$.
iii) On procède par récurrence sur $k$. Si $k=0$, on a $m^k = 1 = (m')^k$, donc $m^0 \equiv (m')^0$ $[b]$. Supposons la propriété vérifiée au rang $k$ : on a $m^{k+1} = m^k.m \equiv (m'^k).m$ $[b]$ (par (ii)) $\equiv (m')^k.m'$ $[b]$ (par (ii) à nouveau) $= (m')^{k+1}$. □

## Critères de divisibilité

Les relations de congruence des entiers relatifs permettent d'établir rigoureusement les critères usuels de divisibilité des entiers naturels par $2, 3, 5, 9$ ou $11$, à partir de leurs chiffres dans leur écriture en base 10 (section 1.7).
On renvoie au Chapitre 2 du cours n° 2 (section sur les multiplets) pour la somme d'un nombre fini quelconque de nombres. Rappelons que la somme $a_1 + \ldots + a_n$ de $n$ entiers relatifs ($n \in \mathbb{N}$), notée de manière plus scientifique $\sum_{i=1}^{n} a_i$, est définie par récurrence sur $n$ par $a_1 + \ldots + a_n = 0$ si $n = 0$, et $a_1 + \ldots + a_{n+1} = (a_1 + \ldots + a_n) + a_{n+1}$.

**Théorème 2.7.6.** *Soient $n$ un entier naturel et $\sum_{i=0}^{k} n_i.10^i$ sa décomposition en base 10 par le théorème 1.7.6, de sorte que $n_0$ est le* chiffre des unités *de $n$.*
*i) L'entier $n$ est pair si et seulement si $n_0$ est pair.*
*ii) L'entier $n$ est multiple de 5 si et seulement si $n_0$ est multiple de 5.*
*iii) L'entier $n$ est multiple de 3 si et seulement si 3 divise la somme $\sum_{i=0}^{k} n_i$ des chiffres de $n$.*
*iv) L'entier $n$ est multiple de 9 si et seulement 9 divise $\sum_{i=0}^{k} n_i$.*
*v) L'entier $n$ est multiple de 11 si et seulement si 11 divise la somme alternée $\sum_{i=0}^{k}(-n_i)^i = n_0 - n_1 + \ldots + (-1)^k n_k$ des chiffres de $n$.*

*Démonstration.* i) On a $10 \equiv 0$ $[2]$, donc $10^i \equiv 0^i = 0$ $[2]$ pour tout $i$ par la proposition 2.7.5, si bien que par récurrence sur $k$, on a $n = \sum_{i=0}^{k} n_i.10^i \equiv n_0$ $[2]$. Autrement dit, on a $2|n$ si et seulement si $2|n_0$, c'est-à-dire si et seulement si $n_0 = 0, 2, 4, 6$ ou $8$.
ii) Comme $10 \equiv 0$ $[5]$, par le même raisonnement qu'en (i) on a $n = \sum_{i=0}^{k} \equiv n_0$ $[5]$, donc $n$ est multiple de 5 si et seulement si $n_0$ l'est.
iii) On a $10 \equiv 1$ $[3]$, puisque $3|10-1=9$, donc $10^i \equiv 1$ $[3]$ pour tout $i \in \mathbb{N}$ par 2.7.5 à nouveau, d'où $n = \sum_{i=0}^{k} n_i.10^i \equiv \sum_{i=0}^{k} n_i$, ce qu'il faudrait montrer par récurrence sur $k$ à nouveau. On a donc $3|n$ si et seulement si $3|\sum_{i=0}^{k} n_i$.
iv) On applique exactement le même raisonnement qu'au (iii).
v) On a $11 = 10-(-1)$, donc par définition $10 \equiv -1$ $[11]$, si bien que $10^i \equiv (-1)^i$ $[11]$ pour tout $i \in \mathbb{N}$ encore par 2.7.5, et $n = \sum_{i=0}^{k} \equiv \sum_{i=0}^{k} n_i.(-1)^i$ $[11]$. Le membre de droite est $\sum_{i=0}^{k}(-n_i)^i$, par les règles de calcul sur les puissances, d'où le résultat. □

**Exemple 2.7.7.** i) L'entier 111111 est divisible par 11, puisque la somme alternée de ses chiffres est nulle. Il est également divisible par 3 puisque la somme de ses chiffres est 6, mais pas par 9. En revanche, selon la même analyse l'entier 333333 est divisible par 11 et par 9 (puisqu'on multiplie par 3 la somme des chiffres de 111111), donc par 99 puisque 11 et 9 sont premiers entre eux.

ii) La somme des chiffres de l'entier 123456789 est 45 : il est donc divisible par 5 et par 9, mais pas par 2. La somme alternée de ses chiffres est 5, donc il n'est pas divisible par 11.

### 2.7.2 Quelques résultats fondamentaux

Nous allons illustrer l'intérêt des relations de congruences par quelques théorèmes élémentaires d'arithmétique modulaire. Le premier est fondamental et existe sous de nombreuses formes.

**Théorème 2.7.8** (Théorème chinois des restes)**.** *Soient $m, n$ deux entiers naturels supérieurs à 2 et premiers entre eux. Pour tous entiers relatifs $a$ et $b$, il existe alors un entier $x$ tel que $x \equiv a\ [m]$ et $x \equiv b\ [n]$.*

*Démonstration.* Par le théorème de Bézout, comme $m$ et $n$ sont premiers entre eux il existe $u, v \in \mathbb{Z}$ tels que $um + vn = 1$, d'où $vn - 1 = um$, si bien que $m \mid vn - 1$; on a aussi $um - 1 = -vn$, si bien que $n \mid um - 1$. On a donc $vn \equiv 1\ [m]$ et $um \equiv 1\ [n]$. Par ailleurs, on a aussi trivialement $vn \equiv 0\ [n]$ et $um \equiv 0\ [m]$, si bien que $aum + bvn \equiv a\ [n]$ et de même $aum + bvn \equiv b\ [m]$, par la proposition 2.7.5 : l'entier $x = aum + bvn$ convient. □

**Remarque 2.7.9.** i) Par récurrence, on peut démontrer une version plus générale de ce théorème, pour un ensemble fini de conditions de congruences données (voir les exercices).

**Exemple 2.7.10.** Cherchons un entier $x$ tel que $x \equiv 2\ [11]$ et $x \equiv 3\ [9]$. On peut chercher une relation de Bézout entre 9 et 11 par l'algorithme d'Euclide : on a $11 = 9.1+2$ et $9 = 2.4+1$, d'où $2 = 11-9$ et $1 = 9-4.2 = 9-4.(11-9) = 9.5+11.(-4)$, ce qu'on peut deviner aussi directement. L'entier $x = 3.(-44) + 2.(45) = -42$ répond à la question.

L'autre théorème élémentaire que nous voulons démontrer est le petit théorème de Fermat, dont la version la plus simple, présentée ici, a trait aux congruences des puissances des entiers par un nombre premier.

**Lemme 2.7.11.** *Si $p$ est un entier naturel premier et $k \in \{1, \ldots, p-1\}$, alors $p$ divise $C_p^k$.*

*Démonstration.* Par définition (voir le Chapitre 3 du cours n° 2) on a $C_p^k = \dfrac{p!}{k!(p-k)!}$, soit $p! = k!(p-k)!C_p^k$. Comme $k \in \{1, \ldots, p-k\}$, on a $k, p-k < p$, donc $p$ ne divise ni $k!$ ni $(p-k)!$ (sinon, par le lemme d'Euclide 2.5.6 $p$ diviserait l'un de leurs facteurs, strictement inférieur à $p$). Par le lemme d'Euclide à nouveau, il s'ensuit que $p \mid C_p^k$. □

**Théorème 2.7.12** (Petit théorème de Fermat)**.** *Si $m$ est un entier relatif et $p$ un entier naturel premier, alors on a $m^p \equiv m\ [p]$.*

*Démonstration.* Distinguons deux cas, selon que $p = 2$ ou $p \neq 2$. Si $p = 2$, alors $m^2 - m = m(m-1)$ est le produit de deux entiers consécutifs, dont l'un au moins est pair : c'est donc un nombre pair, c'est-à-dire que $2|m^2 - m$, ou encore $m^2 \equiv m\ [2]$. Supposons que $p$ est impair. Montrons d'abord par récurrence que la congruence est vérifiée pour tout $m \in \mathbb{N}$. Si $m = 0$, on a $m^p = 0^p = 0$, donc $m^p - m = 0$ et comme $p \mid 0$, on a $m^p \equiv m\ [p]$. Supposons par hypothèse de récurrence que $m \in \mathbb{N}$ et que $m^p \equiv m\ [p]$, et écrivons $(m+1)^p = m^p + \sum_{k=1}^{p-1} C_p^k m^k + 1$, par la formule du binôme de Newton (cours n° 2, Chapitre 3). Par le lemme 2.7.11, pour tout $k = 1, \ldots, p-1$ on a $p \mid C_p^k$, d'où $C_p^k m^k \equiv 0\ [p]$ et finalement, on a $(m+1)^p \equiv m^p + 1\ [p]$ par la proposition 2.7.5. Par l'hypothèse de récurrence, on a $m^p + 1 \equiv m + 1\ [p]$, d'où finalement $(m+1)^p \equiv m + 1\ [p]$, ce qui est la propriété au rang $m+1$, et par récurrence la propriété est vérifiée pour tout $m \in \mathbb{N}$. Soit enfin $m < 0$ : on a $-m \in \mathbb{N}$, donc par ce qui précède on a $(-m^p) \equiv -m\ [p]$. Comme $p$ est impair, on a aussi $(-1)^p = -1$, si bien que $m^p = (-1)^p.(-m)^p \equiv (-1).(-m) = m\ [p]$, et le théorème est démontré. □

**Corollaire 2.7.13.** *Si $p$ est un nombre premier et $x$ un entier relatif premier à $p$, alors $x^{p-1} \equiv 1\ [p]$.*

*Démonstration.* Par le théorème 2.7.12, on a $p \mid x^p - x = (x^{p-1} - 1)x$; comme $p$ est premier et $p \nmid x$ par hypothèse, on a donc $p|x^{p-1} - 1$ par le lemme d'Euclide 2.5.6, c'est-à-dire $x^{p-1} \equiv 1\ [p]$. □

**Exemple 2.7.14.** On a $1024 = 2^{10} \equiv 1\ [11]$ par le corollaire 2.7.13, donc $11|1023$, ce que nous savons aussi par le critère de divisibilité par 11.

Ces théorèmes trouveront des interprétations structurelles fondamentales dans le cours élémentaire de théorie des anneaux (Semestre II).

## Exercices de la section

*Exercice* 2.7.15. i) Démontrer la clause (iv) du théorème 2.7.6.
ii) Démontrer que $625 \equiv 4\ [3]$ et que $753 \equiv 5\ [11]$.
iii) Démontrer par récurrence sur $n \in \mathbb{N}$, $n \geq 2$, la version générale suivante du théorème chinois 2.7.8 : si $a_1, \ldots, a_n$ sont $n$ entiers naturels supérieurs à 2, et si $b_1, \ldots, b_n$ sont $n$ entiers relatifs quelconques, alors il existe un entier $x$ tel que $x \equiv b_i\ [a_i]$ pour $i = 1, \ldots, n$.
iv) Démontrer que $9\ 999\ 999 \equiv 2\ [7]$. Indication : travailler avec les puissances de 10 et utiliser le fait que 7 est premier.
v) Démontrer que 47 est congru à 567 modulo 5. Démontrer que 1113 est congru à 178 modulo 17; quels sont tous les entiers naturels $b > 0$ pour lesquels ces deux nombres sont congrus modulo $b$ ?

# Chapitre 3

# L'ensemble $\mathbb{Q}$ des nombres rationnels

Dans le Chapitre 2, nous avons abordé l'axiomatisation de l'ensemble $\mathbb{Z}$ des nombres entiers relatifs, comme "extension" de l'ensemble $\mathbb{N}$ des nombres entiers naturels, à partir d'une description de l'addition dans $\mathbb{Z}$. Les propriétés de l'addition, de la multiplication, de l'ordre naturel et de la divisibilité dans $\mathbb{Z}$ ont alors été établies à partir des propriétés de leurs contreparties dans $\mathbb{N}$ (dérivant elles-mêmes des axiomes de Peano), et des deux axiomes de l'addition dans $\mathbb{Z}$. Ainsi, nous avons pu approfondir de manière substantielle l'arithmétique élémentaire grâce à l'opération de soustraction, et fonder par là ce premier étage de la théorie des nombres sur quelques cinq axiomes assez simples.
Dans ce chapitre, nous poursuivons notre approche scientifique de la théorie des ensembles naturels de nombres par la description, à nouveau axiomatique, de l'ensemble $\mathbb{Q}$ des nombres rationnels, et par l'extension de concepts et propriétés arithmétiques déjà évoqués pour les ensembles $\mathbb{N}$ et $\mathbb{Z}$. Nous prolongerons également la "structure naturelle" (addition, multiplication et ordre), de $\mathbb{Z}$ à $\mathbb{Q}$, avec une exception notable, celle de la divisibilité : par définition, cette relation ne présente plus aucun intérêt dans $\mathbb{Q}$, si bien qu'il nous faut considérer d'autres manière d'aborder l'arithmétique des nombres rationnels, notamment à travers les "valuations", généralisations des exposants des nombres premiers.
Dans l'ensemble $\mathbb{Q}$ apparaissent également, par "densité" de l'ordre, les premières notions et propriétés géométriques, qui sont ici essentiellement associées aux notions et propriétés arithmétiques, ce qui nous permettra d'entrer de plain pied dans la géométrie au cours suivant. C'est notamment l'occasion de parler de *commensurabilité*, l'analogue rationnel de la recherche du plus grand diviseur commun, qui illustre une forme de "passage" de l'arithmétique à la géométrie.

## 3.1 Description axiomatique de l'ensemble $\mathbb{Q}$

Comme nous l'avons fait pour l'ensemble $\mathbb{N}$ et pour l'ensemble $\mathbb{Z}$, nous admettons ici l'existence d'un ensemble $\mathbb{Q}$ des nombres rationnels, que nous concevons encore de manière intuitive comme dans le cours n$^o$ 1, et qui contient l'ensemble $\mathbb{Z}$ comme sous-ensemble.

Comme pour l'ensemble $\mathbb{Z}$ (Chapitre 2), nous ne démontrons pas "l'existence" de cet ensemble, que nous *construirons* au semestre II, mais nous en donnons une description par des axiomes.

## Axiomatisation de $\mathbb{Q}$ à partir de la multiplication

Dans le Chapitre 1, l'axiomatique de Peano a permis de reconstituer toute la "structure naturelle" de l'ensemble $\mathbb{N}$, essentiellement l'addition puis la multiplication, à partir de la fonction successeur (les relations d'ordre et de divisibilité étant définies à partir des opérations $+$ et $\times$). Dans le Chapitre 2, c'est à partir de l'addition que nous avons axiomatisé l'ensemble $\mathbb{Z}$, pour définir ensuite la multiplication des entiers relatifs à partir de leur addition et de la multiplication des entiers naturels. En effet, la différence essentielle entre les ensembles $\mathbb{N}$ et $\mathbb{Z}$, c'est que dans $\mathbb{Z}$ on peut *opposer* tout élément, autrement dit *soustraire* les nombres.
Dans ce troisième et dernier chapitre, c'est à partir de la *multiplication* que nous axiomatisons l'ensemble $\mathbb{Q}$, pour définir ensuite l'addition, à partir de l'addition des entiers relatifs et de la *division*. La différence essentielle entre les ensemble $\mathbb{Z}$ et $\mathbb{Q}$ réside en effet dans la possibilité d'*inverser* tout nombre non nul, et donc de diviser par un tel nombre.
Nous admettons donc l'existence d'une application de multiplication $\times : \mathbb{Q}\times\mathbb{Q} \to \mathbb{Q}$, prolongeant la multiplication des entiers relatifs, et possédant les propriétés axiomatiques suivantes (à comparer avec l'axiome 2.1.1) :

**Axiome 3.1.1.** *i) Pour tout $r \in \mathbb{Q}$, on a $1.r = r$*
*ii) Pour tous $q, r \in \mathbb{Q}$, on a $q.r = r.q$ (la multiplication est commutative)*
*iii) Pour tous $q, r, s \in \mathbb{Q}$, on a $(q.r).s = q.(r.s)$ (la multiplication est associative)*
*iv) Pour tout $r \in \mathbb{Q}$,* non nul, *il existe $q \in \mathbb{Q}$ tel que $r.q = 1$ (tout élément non nul possède un inverse pour la multiplication).*

**Remarque 3.1.2.** Dire que la multiplication des nombres rationnels *prolonge* celle des entiers relatifs, cela signifie que pour $n, m \in \mathbb{Z}$, le résultat de l'opération $n.m$ dans $\mathbb{Q}$ (puisque $\mathbb{Z} \subseteq \mathbb{Q}$) est le produit $n.m$ tel qu'il a été défini à la section 1.2, ou encore, que la multiplication $\times_{\mathbb{Z}} : \mathbb{Z}^2 \to \mathbb{Z}$ des entiers relatifs est la restriction de $\times$ à $\mathbb{Z}$, soit $\times_{\mathbb{Z}} = \times|_{\mathbb{Z}}$.

Par la propriété (iv) de l'axiome 3.1.1, tout nombre rationnel non nul possède un *inverse* pour la multiplication : c'est la propriété fondamentale que ne possède pas l'ensemble $\mathbb{Z}$ et qui fait l'intérêt arithmétique et géométrique de l'ensemble $\mathbb{Q}$.
L'inverse (multiplicatif) $q$ d'un nombre rationnel $r$ est nécessairement unique : en effet, si $s \in \mathbb{Q}$ et $r.s = 1$, alors on a $q = 1.q$ (par (i)) $= q.1$ (par (ii)) $= q.(r.s) = (q.r).s$ (par (iii)) $= (r.q).s$ (par (ii)) $= 1.s = s.1$ (par (ii)) $= s$ (par (i)). On note $1/r$ ou $\dfrac{1}{r}$ l'inverse de $r$, et on *définit* le **quotient** $r/s$ de deux nombres rationnels $r$ et $s$, avec $s \neq 0$, comme le nombre rationnel $r \times (1/s)$.

**Définition 3.1.3.** L'application $/ : \mathbb{Q}\times\mathbb{Q}^* \to \mathbb{Q}$, qui associe à un couple de nombres rationnels $(r, s)$, avec $s$ non nul, le quotient $r/s = r.(1/s)$, est la *division* des nombres rationnels. On rappelle que $\mathbb{Q}^*$ est l'ensemble des nombres rationnels non nuls.

Les propriétés de l'axiome 3.1.1 ne suffisent pas à caractériser l'ensemble $\mathbb{Q}$, c'est-à-dire à le décrire de manière essentiellement unique. Pour compléter cette description axiomatique, il nous faut introduire un axiome fondamental, analogue à l'axiome 2.1.4, qui permet de situer les nombres rationnels par rapport aux entiers relatifs :

**Axiome 3.1.4.** *Pour tout nombre rationnel $r$, il existe un entier naturel $d$ tel que $r.d$ est entier.*

On peut alors démontrer que l'ensemble $\mathbb{Q}$ ainsi décrit est "essentiellement unique". L'axiome 3.1.4 est équivalent à la propriété suivante, qui permet de donner une représentation des nombres rationnels :

**Proposition 3.1.5.** *Si $r$ est un nombre rationnel, alors il existe un entier relatif $a$ et un entier relatif $b$ non nul, tels que $r = a/b$, et on peut toujours supposer que $b$ est un entier naturel.*

*Démonstration.* Par l'axiome 3.1.4, il existe un entier naturel $d$ tel que $r.d \in \mathbb{Z}$. Posons $a = r.d$ : on a $a/d = a.(1/d) = (r.d).(1/d) = r.(d.(1/d)) = r.1$ (par définition de l'inverse) $= r$, si bien que $a = r.d$ et $b = d$ conviennent, puisque $d$ est un entier naturel. □

La figure 14 propose une représentation géométrique des nombres rationnels comme droites vectorielles du plan passant par des points à coordonnées entières (voir le cours n° 4).
Le quotient $a/b$ d'un entier relatif par un entier relatif non nul est donc toujours défini comme nombre rationnel, et inversement un nombre rationnel peut donc toujours s'écrire sous la forme d'un quotient $a/b$, où $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$ : les nombres rationnels sont donc toutes les "fractions" de la forme $a/b$, pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.
Cependant, une telle écriture d'un nombre rationnel n'est jamais unique : par exemple, le nombre rationnel $1/2$ s'écrit aussi sous la forme $(-7)/(-14)$ et en général sous la forme $n/2n$ pour tout entier relatif $n$ non nul. En fait, si $r$ est un nombre rationnel et $r = a/b$, pour tout nombre entier relatif $n$ non nul l'entier $n.b$ est non nul par la proposition 2.2.6, si bien qu'on a $r = n.a/n.b$, comme l'indique, parmi d'autres propriétés, la proposition suivante :

**Proposition 3.1.6.** *i) Si $a$ et $b$ sont deux entiers relatifs non nuls, on a $1/ab = (1/a).(1/b)$.*
*ii) Si $r = a/b$ est un nombre rationnel et $n$ est un entier relatif non nul, alors on a $a/b = na/nb$.*
*iii) Si $a, b, c, d$ sont des entiers relatifs et $b, d \neq 0$, on a $a/b = c/d$ si et seulement si $ad = cb$.*

*Démonstration.* i) Par définition, $1/ab$ est l'unique nombre rationnel $r$ tel que $(ab).r = 1$. Or, on a $(ab).((1/a).(1/b)) = a.b.(1/b).(1/a)$ (par les propriétés de la multiplication) $= a.(1/a)$ (puisque $b.(1/b) = 1$) $= 1$, d'où $1/ab = (1/a).(1/b)$.
ii) On a $na/nb = (na).(1/nb)$ (par définition de la division) $= (na).((1/n).(1/b))$ (par (i)) $= a.n.(1/n).(1/b) = a.(1/b) = a/b$.
iii) Supposons que $a/b = c/d$ : on a $a.(1/b) = c.(1/d)$, et en multipliant chaque membre par $bd$, on obtient par les propriétés de la multiplication $a.d = a.(1/b).b.d =$

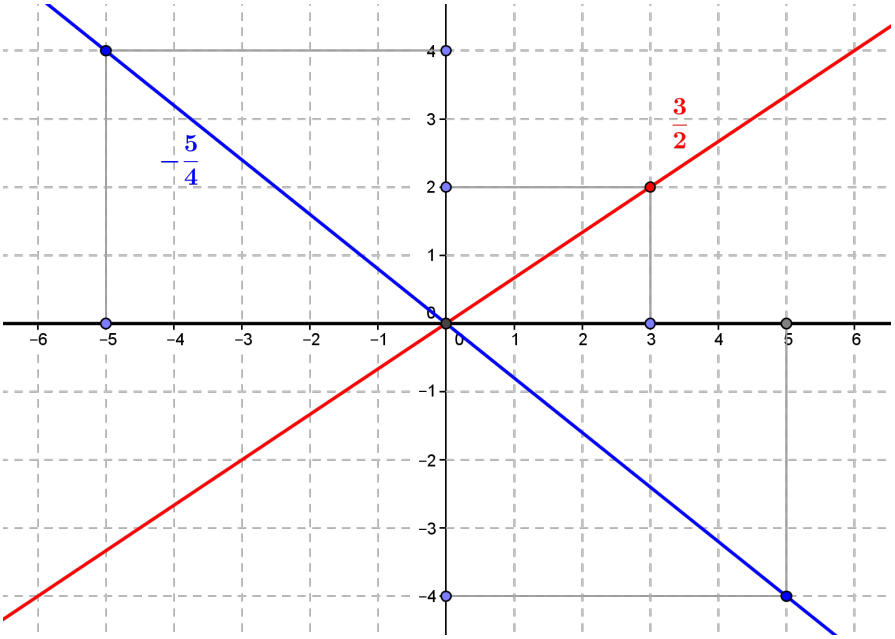



Figure 14: On peut représenter les nombres rationnels comme les droites du plan passant par l'origine et un des noeuds du plan (points à coordonnées entières), en exceptant la droite que représente l'axe des abscisses (en noir) et qui correspond à un dénominateur nul. Plusieurs noeuds du plan (couples d'entiers équivalents) définissent le même nombre rationnel, en particulier les points opposés (exemple de la droite en bleu).

$c.(1/d).b.d = c.(1/d).d.b = c.b$. Inversement, si $ad = cb$, comme $bd \neq 0$ par la proposition 2.2.6 on peut diviser les deux membres par $bd$ pour obtenir $a/b = ad/bd$ (par (ii)) $= ad.(1/bd) = ad.(1/b).(1/d)$ (par (i)) $= cb.(1/b).(1/d) = c.(1/d) = c/d$. □

**Exemple 3.1.7.** Les nombres rationnels $207/(-92)$ et $(-72)/32$ sont égaux, puisque $207 \times 32 = 6624 = (-92).(-72)$.

La caractérisation de l'égalité des nombres rationnels à partir de leurs représentations donnée au (iii) de la proposition 3.1.6 est à la base de la construction que nous donnerons de l'ensemble $\mathbb{Q}$ au deuxième semestre.

### 3.1.1 Formes irréductibles d'un nombre rationnel

Si $r$ est un nombre rationnel et $r = a/b$, le couple $(a, b)$ sera appelé une *représentation de* $r$. Le nombre $a$ est appelé le *numérateur* et $b$ le *dénominateur*, de la représentation. Parmi ces représentations, qui rappelons-le sont en nombre infini (en bijection avec $\mathbb{Z}^*$ par la proposition 3.1.6), il en existe toutefois deux qui sont privilégiées, au sens où elles sont "les plus simples" : il s'agit des *formes irréductibles* du nombre $r$.
En effet, écrivons $r = a/b$ pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Soit $d$ le p.g.c.d de $a$ et $b$ (section 2.4), de sorte qu'on peut écrire $a = \alpha.d$ et $b = \beta.d$, avec $(\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z}^*$ : on a alors $a.\beta.d = ab = ba = b.\alpha.d$, et comme $d \neq 0$, par intégrité de la multiplication dans $\mathbb{Z}$ (proposition 2.2.6), on en déduit que $a.\beta = b.\alpha$, autrement dit que

$r = a/b = \alpha/\beta$. Or, $\alpha$ et $\beta$ sont premiers entre eux (remarque 2.6.12), si bien que nous avons démontré la proposition suivante :

**Proposition 3.1.8.** *Tout nombre rationnel $r$ peut s'écrire sous la forme $a/b$, avec $a$ et $b$ premiers entre eux.*

La représentation d'un nombre rationnel $r$ sous la forme d'une fraction d'entiers relatifs premiers entre eux est donc un choix particulier parmi toutes les représentations possibles. On appelle une telle représentation, qui consiste en le couple $(a, b) \in \mathbb{Z}\times\mathbb{Z}^*$ tel que $r = a/b$, une *forme irréductible* de ce nombre.
Toutefois, il peut exister *a priori* plusieurs formes irréductibles d'un même nombre. Par exemple, le nombre $(-7/23)$ est représenté ici sous forme irréductible puisque $-7$ et 23 sont premiers entre eux, donc le couple $(-7, 23)$ est une telle forme.
Mais on peut aussi l'écrire $7/(-23)$, puisque $(-7).(-23) = 7.23$, donc le couple $(7, -23)$ est une autre forme irréductible ! Ainsi, il existe au moins deux représentations irréductibles de ce nombre et en fait, il n'en existe jamais que deux.

**Proposition 3.1.9.** *Si $r$ est un nombre rationnel non nul, alors il existe exactement deux formes irréductibles de $r$.*

*Démonstration.* L'existence d'une telle forme a été établie précédemment : si $r = a/b$, en simplifiant $a$ et $b$ par leur pgcd on obtient une représentation de $r$ sous forme irréductible. Or, si $(a, b)$ est une forme irréductible de $r$, le couple $(-a, -b)$ donne une autre forme irréductible de $r$ puisque $pgcd(-a, -b) = pgcd(a, b) = 1$, si bien qu'il existe au moins deux telles formes, puisque de toute façon on a $b \neq -b$ (donc $(a, b) \neq (-a, -b)$). Supposons maintenant que $a/b = c/d$, avec $pgcd(a, b) = pgcd(c, d) = 1$. Par définition de $\mathbb{Q}$, on a donc $ad = bc$, et par le lemme de Gauss 2.5.7, on a alors $a|c$ (puisque $a|bc$ et $pgcd(a, b) = 1$) et $c|a$ (puisque $c|ad$ et $pgcd(c, d) = 1$), de sorte que $a = \pm c$. De même, on a $b = \pm d$, si bien qu'on a soit $c/d = a/b$ (dans le cas où $a = c$), soit $c/d = (-a)/(-b)$ (dans le cas où $b = d$), et les deux formes irréductibles $(a, b)$ et $(-a, -b)$ sont donc les seules possibles. □

**Remarque 3.1.10.** Nous n'avons défini *stricto sensu* le p.g.c.d de deux entiers relatifs que s'ils sont tous deux non nuls. Cependant, la définition s'étend naturellement au cas où l'un seulement est non nul, et permet ainsi d'inclure 0 comme cas particulier de cette proposition : les formes irréductibles de 0 sont $0/1$ et $0/(-1)$.

**Définition 3.1.11.** Si $r$ est un nombre rationnel, sa forme irréductible $(a, b)$ telle que $b > 0$ sera appelée *forme irréductible canonique* de $r$.

L'existence d'une forme irréductible canonique signifie qu'on peut toujours choisir, dans l'écriture fractionnaire d'un nombre rationnel, le dénominateur comme un entier naturel.

## Exercices de la section

*Exercice* 3.1.12. i) Les nombres rationnels $\dfrac{110}{273}$ et $\dfrac{1431}{3529}$ sont-ils égaux ? Sinon, corriger le numérateur ou le dénominateur d'un des deux nombres pour obtenir deux fractions égales.

ii) Mettre sous forme irréductible canonique les nombres $\frac{30}{-105}$, $\frac{-231}{182}$ et $\frac{378}{1980}$.
iii) En utilisant des décompositions en nombres premiers, multiplier $-42/65$ par $286/231$.

## 3.2 Extension de la structure arithmétique de l'ensemble $\mathbb{Z}$

Après avoir décrit de manière axiomatique la multiplication de l'ensemble $\mathbb{Q}$ de manière à déterminer celui-ci de manière univoque, nous procédons maintenant à l'extension du reste de la structure arithmétique (pure) de l'ensemble $\mathbb{Z}$ à l'ensemble $\mathbb{Q}$, en définissant l'addition, la division et la soustraction de nombres rationnels.

### 3.2.1 Réduction au même dénominateur

Etant donnés deux nombres rationnels $r = a/b$ et $s = c/d$ sous forme de fractions, en général les dénominateurs de celles-ci sont différents, c'est-à-dire $b \neq d$.

**Définition 3.2.1.** On dit qu'on a *réduit $r$ et $s$ au même dénominateur*, si il existe un entier relatif (non nul) $e$ et des représentations $r = a'/e$ et $s = c'/e$ ayant le même nombre $e$ comme dénominateur.

Il est toujours possible de réduire les deux fractions $r$ et $s$ au même dénominateur : la manière la plus directe de procéder est d'obtenir $e$ comme le produit des deux dénominateurs, c'est-à-dire de poser $e = b.d$, entier non nul par intégrité de la multiplication dans $\mathbb{Z}$ (2.2.6). On obtient alors $r = a/b = ad/bd = ad/e$ et $s = c/d = bc/bd = bc/e$.
Mais trouver un dénominateur commun à deux nombres rationnels revient en fait à trouver un multiple commun à leurs deux dénominateurs. Or, si le produit des deux dénominateurs est un choix naturel, il existe toutefois un "meilleur choix" donné par le plus petit commun multiple, qui est toujours un entier naturel (section 2.6).

**Proposition 3.2.2.** *Si $r = a/b$ et $s = c/d$ sont deux nombres rationnels et $e = ppcm(b, d)$, alors il existe deux représentations de la forme $r = a'/e$ et $s = c'/e$. De plus, si les représentations $r = a/b$ et $s = c/d$ sont irréductibles, alors $e$ est le "plus petit dénominateur commun" à $r$ et $s$ au sens de la divisibilité.*

*Démonstration.* Par définition du p.p.c.m (2.6.13) et par la proposition 2.6.11, il existe $u, v \in \mathbb{Z}$ tels que $e = ub = vd$, d'où $r = a/b = ua/ub = ua/e$ et $s = c/d = vc/vd = vc/e$, d'où l'existence des deux représentations avec $a' = ua$ et $c' = vc$. Si $r = x/e'$ et $s = y/e'$ sont deux autres représentations avec un dénominateur commun, supposons que $r = a/b$ et $s = c/d$ sont deux représentations irréductibles et conservons les mêmes notations : on a $xb = ae'$ (puisque $r = a/b = x/e'$) et $yd = ce'$ (puisque $s = c/d = y/e'$). Puisque $a$ et $b$ sont premiers entre eux par irréductibilité, on a alors $b|e'$; de même, on a $c|e'$, et par caractérisation du p.p.c.m (2.6.11), on a $e|e'$, ce qu'il fallait démontrer. □

Ainsi, l'expression populaire "trouver le plus petit dénominateur commun", utilisée métaphoriquement, correspond à la recherche du "meilleur" dénominateur positif commun de deux fractions données sous forme irréductible. Mais si les nombres rationnels ne sont pas donnés sous forme irréductible, il faut ajouter une étape pour aboutir à cette représentation.

**Exemple 3.2.3.** Réduisons les fractions $\frac{-517}{1960}$ et $\frac{3215}{126}$ au même dénominateur : par exemple, on décompose $1960 = 2^3.5.7^2$ et $126 = 2.3^2.7$ en nombres premiers; leur p.p.c.m est $2^3.3^2.5.7^2 = 17640$ par la proposition 2.6.15, donc $\frac{-517}{1960} = \frac{(-517).3^2}{17640} = \frac{-4653}{17640}$, tandis que $\frac{3215}{126} = \frac{3215.2^2.5.7}{17640} = \frac{450100}{17640}$.

### 3.2.2 Définition algébrique de l'addition des nombres rationnels

Lorsque nous avons axiomatisé l'ensemble $\mathbb{Z}$ dans le Chapitre 2, nous avons utilisé l'addition, puis nous avons *défini* la multiplication des entiers relatifs à partir de la structure axiomatique de $\mathbb{Z}$. Ici, nous avons plutôt axiomatisé l'ensemble $\mathbb{Q}$ à partir de la multiplication : par analogie, nous pouvons désormais *définir* l'addition des nombres rationnels à partir de la structure axiomatique évoquée à la section 3.1 et de la réduction au même dénominateur :

**Définition 3.2.4.** Soient $r = a/b$ et $s = c/d$ deux nombres rationnels, avec $a, b, c, d \in \mathbb{Z}$. On définit la *somme de $r$ et $s$* comme le nombre rationnel noté $r + s$ ou $\frac{a}{b} + \frac{c}{d}$, et égal au quotient $\dfrac{ad + bc}{bd}$.

Ainsi, on définit de cette manière une application de $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, *l'addition* des nombres rationnels $+ : (a/b, c/d) \mapsto (ad + bc)/bd$. Cependant, comme dans la section 2.2.1, la définition posée ici de la somme $r+s$ dépend *a priori* d'un choix de représentation des nombres $r$ et $s$ (ici comme quotients de nombres entiers relatifs). Nous devons donc à nouveau vérifier que ce n'est pas le cas, autrement dit que le choix d'autres représentations de $r$ et $s$ conduit au même résultat :

**Proposition 3.2.5.** *Si $r = a/b = a'/b'$ et $s = c/d = c'/d'$, alors on a $(a'd' + b'c').bd = (ad + bc).b'd'$, donc la somme de $r$ et $s$ est bien définie.*

*Démonstration.* Par hypothèse, on a $ab' = a'b$ et $cd' = c'd$ par la proposition 3.1.6(iii). Il vient $(a'd' + b'c').bd = a'd'bd + b'c'bd = a'bdd' + c'dbb' = ab'dd' + cd'bb' = adb'd' + bcb'd' = (ad + bc).b'd'$, par les propriétés de la multiplication dans $\mathbb{Z}$. On en déduit que $(ad + bc)/bd = (a'd' + b'c')/b'd'$, donc que l'addition de $r$ et $s$ est bien définie. □

En considérant $\mathbb{N}$ comme sous-ensemble de $\mathbb{Z}$, nous avons identifié au Chapitre 2 le "zéro" de $\mathbb{N}$ et celui de $\mathbb{Z}$, pour axiomatiser l'addition. Pour pouvoir considérer que l'ensemble $\mathbb{Q}$ est une extension de l'ensemble $\mathbb{Z}$ "qui préserve sa structure arithmétique", il faut en particulier que le zéro de $\mathbb{N}$ et de $\mathbb{Z}$ soit aussi celui de l'addition des nombres rationnels, ce que nous vérifions ici avec les autres propriétés élémentaires usuelles de l'addition dans $\mathbb{Q}$, analogues à celles de l'addition dans $\mathbb{Z}$.

**Proposition 3.2.6.** *Soient $q, r$ et $s$ trois nombres rationnels.*
*o) On a $q + 0 = q$*
*i) On a $q + r = r + q$ (l'addition est commutative)*
*ii) On a $(q + r) + s = q + (r + s)$ (l'addition est associative)*
*iii) On a $q.(r + s) = q.r + q.s$ (la multiplication est distributive sur l'addition).*

*Démonstration.* Ces propriétés découlent de la description axiomatique de $\mathbb{Q}$ et des définitions et des propriétés des opérations analogues dans $\mathbb{Z}$. Posons $q = a/b$, $r = c/d$ et $s = e/f$, avec $a, c, e \in \mathbb{Z}$ et $b, d, f \in \mathbb{Z}^*$.
o) Par définition, on a $q + 0 = a/b + 0/1 = (a.1 + 0.b)/b.1 = a/b = q$.
i) Par définition, on a $q+r = a/b+c/d = (ad+bc)/bd = (cb+da)/db = c/d+a/b = r + q$.
ii) On a $(q+r)+s = (a/b+c/d)+e/f = (ad+bc)/bd+e/f = ((adf+bcf)+bde)/bdf = (adf + (bcf + bde))/bdf = a/b + (cf + de)/df = a/b + (c/d + e/f) = q + (r + s)$.
iii) Par définition, on a $q.(r + s) = (a/b).((c/d) + (e/f)) = (a/b).((cf + de)/df) = (acf+ade)/bdf = acf/bdf+ade/bdf = ac/bd+ae/bf = (a/b).(c/d)+(a/b).(e/f) = q.r + q.s$. □

### 3.2.3 Soustraction des nombres rationnels

Dans la construction de $\mathbb{Z}$, nous avons ajouté des opposés additifs à tous les entiers naturels, et tout entier relatif possède un opposé additif : c'était la motivation initiale de la construction. En passant de $\mathbb{Z}$ à $\mathbb{Q}$, l'existence des opposés est préservée : si $a/b$ est un nombre rationnel, on a par définition $a/b + (-a)/b = (a.b + b.(-a))/b^2 = 0/b^2 = 0$, si bien que $(-a)/b$ est un opposé pour $a/b$.
Montrons qu'il n'existe qu'un seul opposé possible : si $c/d$ est un nombre rationnel tel que $a/b + c/d = 0$, alors par définition on a $0/1 = (ad + bc)/bd$, c'est-à-dire $0 = 0.(bd) = 1.(ad + bc) = ad + bc$, d'où $-ad = bc$, c'est-à-dire $(-a)/b = c/d$ par la proposition 3.1.6. On peut donc parler de l'opposé (au singulier) de $a/b$, qu'on note $-a/b$ ou $-\frac{a}{b}$.

**Définition 3.2.7.** Si $a/b$ et $c/d$ sont deux nombres rationnels, la *différence* de $a/b$ et $c/d$ est le nombre rationnel $a/b + (-c/d)$, soit $(ad - bc)/bd$. La *soustraction* des nombres rationnels est l'application $- : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, $(a/b, c/d) \mapsto a/b - c/d$.

La soustraction des nombres rationnels possède les mêmes propriétés universelles élémentaires que celle des entiers relatifs. L'essentiel est de retenir la règle suivante, associée à la multiplication :

**Proposition 3.2.8.** *Si $a/b$ est un nombre rationnel, alors $(-1).(a/b) = -a/b$.*

*Démonstration.* Nous pouvons écrire $-1$, en tant que nombre rationnel, comme le quotient $(-1)/1$, si bien que $(-1).(a/b) = ((-1)/1).(a/b) = ((-1).a)/(1.b) = (-a)/b = -a/b$. □

### 3.2.4 Division et inversion des nombres rationnels

La construction de $\mathbb{Q}$ permet d'écrire des quotients de nombres entiers relatifs, c'est-à-dire d'obtenir de nouveaux nombres qui sont le résultat de la division d'un entier

relatif par un entier relatif non nul quelconque, alors que la division dans $\mathbb{Z}$ n'est possible que dans certains cas très particuliers (par 1 ou par $-1$). Ceci étant dit, comme pour l'existence des opposés dans $\mathbb{Z}$, la construction ne garantit pas *a priori* que l'on puisse toujours diviser un nombre rationnel par un nombre rationnel non nul. C'est pourtant le cas :

**Proposition 3.2.9.** *Si $p$ et $q$ sont deux nombres rationnels avec $q$ non nul, alors il existe un unique nombre rationnel $r$ tel que $r.q = p$. On note ce nombre $p/q$ ou $\frac{p}{q}$.*

*Démonstration.* Ecrivons $p = a/b$ et $q = c/d$ avec $a, c \in \mathbb{Z}$ et $b, d \in \mathbb{Z}^*$, de sorte que $c \neq 0$ par l'hypothèse et la proposition 3.1.6. Si $r = e/f$ est un nombre rationnel, avec $e \in \mathbb{Z}$ et $f \in \mathbb{Z}^*$, et tel que $r.q = p$, on a $ec/fd = a/b$, si bien que $ecb = fda$ par 3.1.6 à nouveau, d'où nécessairement $r = e/f = ebc/fbc = fad/fbc = ad/bc$, puisque $bc \neq 0$ par intégrité de la multiplication dans $\mathbb{Z}$ (proposition 2.2.6). Or, on a bien $(ad/bc).(c/d) = adc/bcd = a/b = p$, donc $ad/bc$ convient; par ce qui précède, c'est le seul nombre ayant cette propriété. □

**Remarque 3.2.10.** Cette démonstration est un exemple typique de la méthode dite *d'analyse-synthèse* : pour montrer l'existence d'un objet ayant une certaine propriété, on déduit de cette propriété les caractéristiques que doit nécessairement posséder un tel objet (phase d'analyse), ce qui permet de l'identifier ou de le construire, puis on vérifie que l'objet identifié possède la propriété demandée (phase de synthèse). Cette méthode est souvent utilisée pour résoudre des équations ou des systèmes d'équations.

Lorsque nous écrirons le quotient $p/q$ de deux nombres rationnels, et que $p$ ou $q$ est un entier relatif, nous utiliserons souvent l'écriture de ce dernier comme entier relatif, sans utiliser de fraction. Par exemple, pour dénoter le résultat de la division d'un nombre rationnel $p$ par 2, nous écrirons $p/2$ et pas $p/(2/1)$. Ou encore, pour dénoter le résultat de la division de 3 par un nombre rationnel $q$, nous écrirons $3/q$ et pas $(3/1)/q$.
La proposition 3.2.9 permet d'établir directement l'existence d'un *inverse* pour tout nombre rationnel non nul : c'est en fait l'intérêt principal de la construction, qui fait de $\mathbb{Q}$ un *corps*, type de structure mathématique que nous étudierons au semestre II.

**Corollaire 3.2.11.** *i) Tout nombre rationnel non nul possède un unique inverse. Autrement dit, pour tout $q \in \mathbb{Q}^*$, il existe un unique $r \in \mathbb{Q}^*$, noté $1/q$, tel que $q.r = 1$.*
*ii) Si $p$ et $q$ sont deux nombres rationnels tels que $p.q = 0$, alors $p = 0$ ou $q = 0$. En particulier, si $p, q, r$ sont trois nombres rationnels et $r$ est non nul, on a $p = q$ dès que $pr = qr$.*
*iii) Pour tous nombres rationnels $p$ et $q$ avec $q \neq 0$, on a $p/q = p.(1/q)$.*

*Démonstration.* i) Pour l'existence unique de $r$, il suffit d'appliquer la proposition 3.2.9 à $p = 1$ : le nombre $r$ cherché est $1/q$.
ii) Si $p.q = 0$, mais $p \neq 0$, alors par (i) on peut inverser $p$ et par définition, on a $0 = (1/p).0 = (1/p).(p.q) = ((1/p).p).q = 1.q = q$, par les propriétés axiomatiques de la multiplication dans $\mathbb{Q}$. Supposons maintenant que $r \in \mathbb{Q}$ n'est pas nul et que $pr = qr$ : on a $0 = pr - qr = (p-q).r$, donc $p - q = 0$ par ce qui précède, soit $p = q$.

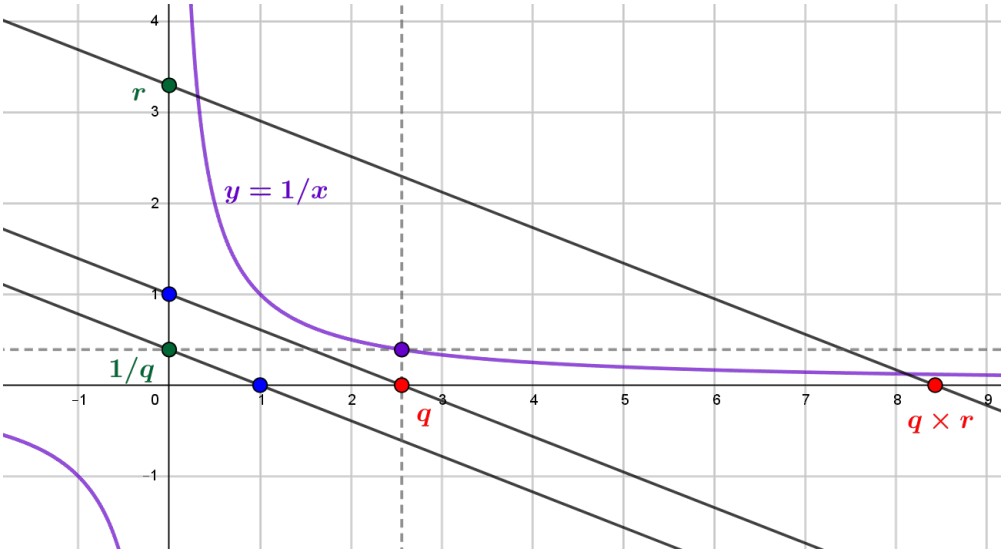



Figure 15: On peut réprésenter la multiplication de nombres rationnels positifs $q$ et $r$ comme dans la figure 8 : le produit $q \times r$ est l'abscisse du point d'intersection avec l'axe des abscisses, de la droite passant par le point $(0, r)$ et parallèle à la droite passant par les points $(q, 0)$ et $(0, 1)$ (!). La même idée permet de représenter l'inverse $1/q$ à partir du point pour lequel la construction précédente donne $q \times r = 1$. En violet, nous avons représenté la fonction $1/x$, qui permet de repérer directement l'inverse de $q$, et que nous étudierons en détail en Analyse. Le cours élémentaire de Géométrie (n° 4) clarifiera toutes ces constructions.

iii) Distinguons deux cas, selon que $p = 0$ ou $p \neq 0$. Si $p = 0$, alors on a $p/q = 0/q = 0$, puisque 0 est le seul nombre rationnel tel que $0.q = 0$. Si $p \neq 0$, par définition on a $q.(p/q) = p$, tandis que $q.(p.(1/q)) = (q.(1/q)).p = 1.p = p$ par les propriétés de la multiplication. Par intégrité de la multiplication dans $\mathbb{Q}$ (clause (ii)), comme $p \neq 0$ on en déduit que $p/q = p.(1/q)$. □

Lorsqu'on écrit le quotient de deux nombres rationnels $p$ et $q$, des représentations de $p$ et $q$ comme fractions de nombres entiers permettent d'obtenir directement une représentation de $p/q$ comme fraction de nombres entiers. En effet, si $p = a/b$ et $q = c/d$ avec $q \neq 0$, l'inverse de $q$ est $d/c$, puisque $c \neq 0$ et $(c/d).(d/c) = cd/cd = 1$. Il s'ensuit qu'on a $p/q = p.(1/q) = (a/b).(d/c) = ad/bc$.

**Exemple 3.2.12.** Divisons le nombre rationnel $p = 27/43$ par le nombre rationnel non nul $q = -101/18$ : on a $p/q = (27 \times 18)/(43 \times (-101)) = -486/4343$.

La figure 15 propose une représentation géométrique de la multiplication de deux nombres rationnels et de l'inversion d'un nombre rationnel, à partir du théorème de Thalès (voir le cours n° 4).

## Exercices de la section

*Exercice* 3.2.13. i) Réduire les fractions $1215/143$ et $-111/65$ au même dénominateur.
ii) Trouver le "plus petit dénominateur commun" aux nombres rationnels $15/(-126)$

et 66/45 et donner une représentation de ces fractions à partir de ce dénominateur.
iii) Additionner 128/165 et 1024/(−187).
iv) Soustraire 28/9 à 17/56.
v) Diviser −79/187 par 2004/(−509).

## 3.3 L'ordre naturel dans $\mathbb{Q}$

### 3.3.1 Prolonger l'ordre naturel de $\mathbb{Z}$ à $\mathbb{Q}$

L'ordre naturel, large ($\leq$) ou strict ($<$), a été défini sur l'ensemble $\mathbb{N}$ à partir de l'addition dans la section 1.3.1, et prolongé à l'ensemble $\mathbb{Z}$ dans la section 2.1. Comme pour les opérations d'addition et de multiplication, on peut prolonger directement l'ordre naturel de l'ensemble des entiers relatifs à l'ensemble des nombres rationnels. L'idée intuitive est que si $a/b$ et $c/d$ sont des nombres rationnels avec $b, d > 0$, alors $a/b > c/d$ si et seulement si $ad > bc$ (en multipliant les deux côtés de la première inégalité par $bd > 0$, on ne devrait pas changer le sens de l'inégalité). Pour le faire de manière tout-à-fait générale, on définit d'abord les éléments *positifs*, en décrétant qu'un nombre rationnel $\frac{a}{b}$ est strictement positif (ce qu'on note $\frac{a}{b} > 0$) si et seulement si le produit $ab$ est strictement positif dans $\mathbb{Z}$. On décrète alors que si $\frac{c}{d}$ est un autre rationnel, on a $\frac{a}{b} < \frac{c}{d}$ si et seulement si $\frac{c}{d} - \frac{a}{b} > 0$. Comme dans le cas de $\mathbb{N}$ et de $\mathbb{Z}$, on définit ainsi un ordre "total" au sens suivant :

**Proposition 3.3.1.** *Soient $a/b$ et $c/d$ deux nombres rationnels. Alors, on a soit $a/b < c/d$, soit $a/b = c/d$, soit $c/d < a/b$, et ces trois possibilités sont mutuellement exclusives.*

*Démonstration.* Les trois propriétés correspondent respectivement, par définition, à $c/d - a/b = (cb - ad)/bd > 0$, $a/b = c/d$ et $a/b - c/d = (ad - bc)/bd > 0$, soit $(cd - ad).bd > 0$, $ad - bc = 0$ et $(ad - bc).bd > 0$. On peut toujours supposer qu'on a choisi $b, d > 0$, si bien que ces possibilités correspondent respectivement à $ad - bc < 0$, $ad - bc = 0$ et $ad - bc > 0$; ce sont toutes les possibilités correspondant à l'entier relatif $ad - bc$ et énumérées dans la proposition 2.1.11, et elles sont mutuellement exclusives par la même proposition. □

Si $n, m \in \mathbb{Z}$, on a $m < n$ dans $\mathbb{Z}$ si et seulement si $n - m > 0$, par la proposition 2.1.10(iii), si et seulement si $\frac{n}{1} - \frac{m}{1} > 0$, si et seulement si $m < n$ dans $\mathbb{Q}$, ce qui justifie à nouveau l'abus de notation consistant à identifier l'ordre naturel dans $\mathbb{Z}$ et dans $\mathbb{Q}$. Comme dans le cas des entiers relatifs, ce prolongement de l'ordre naturel de $\mathbb{Z}$ à $\mathbb{Q}$ est "compatible" avec les opérations arithmétiques d'addition et de multiplication, au sens de la proposition suivante.

**Proposition 3.3.2.** *Soient $q, r$ et $s$ des nombres rationnels.*
*i) Si $q < r$, alors $q + s < r + s$ et $q - s < r - s$.*
*ii) Si $s > 0$ et $q < r$, alors $qs < rs$.*
*iii) Si $s < 0$ et $q < r$, alors $qs > rs$.*
*iv) Si $q > 0$, alors $1/q > 0$, et si $q < 0$, alors $1/q < 0$.*

*Démonstration.* i) Par définition, on a $(r+s)-(q+s) = r+s-q-s = r-q > 0$, si bien que $r+s > q+s$ par définition. La seconde inégalité est obtenue en remplaçant $s$ par $-s$.
ii) Supposons d'abord que $q = 0$, de sorte que $r > 0$, et écrivons $r = a/b$ et $s = c/d$ : par définition, on a $ab > 0$ et $cd > 0$. Dans ce cas, le produit $rs$ vaut $ac/bd$, et comme $(ac).(bd) = (ab).(cd) > 0$ dans $\mathbb{Z}$, on a $rs > 0 = qs$. Dans le cas général, si $q < r$ on a $r-q > 0$ par définition, si bien que par ce qui précède, on a $sr-sq = s.(r-q) > 0$, autrement dit $rs = sr > sq = qs$.
iii) Supposons que $q = 0$ et écrivons à nouveau $r = a/b$ et $s = c/d$ : on a $ab > 0$ et $cd < 0$, d'où $(ac).(bd) = (ad).(bc) < 0$, si bien que $rs < 0$ cette fois-ci. En général, si $q < r$ on a bien $rs - qs = (r-q).s < 0$, d'où $rs < qs$.
iv) Si $q > 0$ et $1/q < 0$, alors $1 = q.(1/q) < 0$ par (iii), contradiction; on en déduit que si $q > 0$, alors $1/q > 0$. De même, si $q < 0$ et $1/q > 0$, on a à nouveau $1 < 0$ par (iii), d'où encore par contradiction, si $q < 0$ on a $1/q < 0$. □

**Remarque 3.3.3.** i) Des relations analogues sont vraies pour l'ordre large, en appliquant directement la définition (voir les exercices).
ii) Lorsque $a/b, c/d \in \mathbb{Q}$ avec $b, d > 0$, d'après la définition on a $a/b < c/d$ si et seulement si $(cb-ad)/bd > 0$, si et seulement si $cb - ad > 0$ par la proposition, puisque $1/bd > 0$ par (iv), ou encore si et seulement si $ad > bc$. Ce critère permet de comparer directement deux fractions par deux multiplications, en se ramenant à des fractions de dénominateur positif, ce qu'on peut toujours faire.

**Exemple 3.3.4.** Certaines fractions sont faciles à comparer sans calcul : par exemple, on a $235/128 > 1$, puisque $128 < 235$, et $49/89 < 1$, puisque $49 < 89$ : on a donc $49/89 < 235/128$. En revanche, on a $49 \times 235 = 11515$ et $128 \times 89 = 11280$, donc $235/128 < 89/49$.

### 3.3.2 Un ordre dense et sans extrémités

L'ordre naturel sur $\mathbb{Z}$ est dit "sans extrémités" : pour tout entier relatif $n$, on a $n < n+1$ (donc il n'y a pas de "plus grand élément", comme dans $\mathbb{N}$), et on a $n-1 < n$ (donc il n'y a pas de "plus petit élément", contrairement à $\mathbb{N}$). Cette propriété reste vraie pour le prolongement de l'ordre naturel à $\mathbb{Q}$ par la proposition 3.3.2 : si $q \in \mathbb{Q}$, on a $q < q+1$ et $q-1 < q$, donc l'ordre naturel sur $\mathbb{Q}$ est également sans extrémités.
En revanche, la propriété suivante, dite de "densité", est prise en défaut dans l'ensemble $\mathbb{Z}$, c'est donc une propriété caractéristique nouvelle de l'ensemble $\mathbb{Q}$ :

**Proposition 3.3.5.** *Si $p$ et $q$ sont deux nombres rationnels tels que $p < q$, alors il existe un nombre rationnel $r$ tel que $p < r < q$.*

*Démonstration.* Considérons par exemple le nombre rationnel $r = \frac{p+q}{2}$, qui représente le milieu du segment $[p,q] = \{x \in \mathbb{Q} : p \leq x \leq q\}$. On a $q - r = q - \frac{p+q}{2} = \frac{2q-p-q}{2} = \frac{q-p}{2} > 0$ par la proposition 3.3.2, puisque $q - p > 0$ par hypothèse. De même, on a $r - p = \frac{p+q-2p}{2} = \frac{q-p}{2} > 0$, donc $r > p$. Finalement, on a $p < r < q$. □

La figure 16 illustre la densité de l'ordre sur l'ensemble $\mathbb{Q}$.

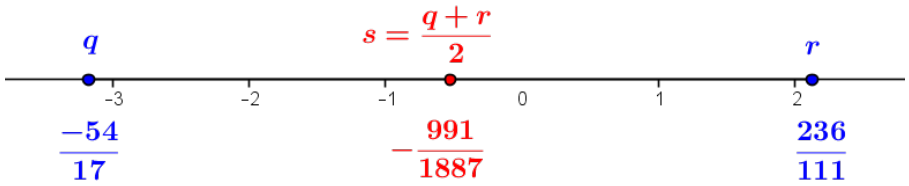



Figure 16: Le nombre rationnel $s = -\frac{991}{1887}$, qui représente le milieu du segment $[q, r]$, est strictement compris entre les nombres rationnels $q = \frac{-54}{17}$ et $r = \frac{236}{111}$.

A ce stade, nous pouvons mentionner la *propriété d'Archimède*, énoncée de manière axiomatique au Chapitre 3 du cours n° 1 pour les nombres réels, mais qui se démontre ici simplement à partir de la division euclidienne :

**Proposition 3.3.6.** *[Propriété d'Archimède] Pour tout nombre rationnel $q$, il existe un nombre entier $n$ tel que $q < n$.*

*Démonstration.* Soit $q \in \mathbb{Q}$, et distinguons deux cas. Si $q < 0$, alors l'entier $n = 0$ convient. Sinon, écrivons $q = a/b$, avec $a, b \geq 0$ : comme $b > 0$, on peut effectuer la division euclidienne de $a$ par $b$ (théorème 1.4.5), sous la forme $a = bq + r$, avec $0 \leq r < b$, de sorte que $a = bq + r < bq + q = b(q + 1)$. Par la proposition 3.3.2, comme $b > 0$ on en déduit que $a/b < q + 1$, donc $n = q + 1$ convient. □

En fait, en reprenant l'idée de la démonstration de la propriété d'Archimède 3.3.6, on peut définir la *partie entière* d'un nombre rationnel sans passer par la "propriété de la mesure" évoquée au Chapitre 5 du cours n° 1.
Soit en effet $r = a/b$ un nombre rationnel quelconque; on peut supposer que $b > 0$, effectuons la division euclidienne de $a$ par $b$ : on peut écrire $a = bq + r$, avec $q, r \in \mathbb{Z}$ tels que $0 \leq r < b$. En ajoutant $bq$ à chaque membre de cette double inégalité, on peut donc écrire l'encadrement $bq \leq a = bq + r < b(q + 1)$, et en divisant les deux inégalités par $b > 0$, par la proposition 3.3.2 à nouveau on obtient

$$q \leq r = a/b < q + 1,$$

de sorte que le quotient $q$ de cette division euclidienne est *le plus grand entier relatif $n$ tel que $n \leq r$*, soit par définition la *partie entière de $r$*.
Nous avons en fait démontré la proposition suivante, qui établit un lien explicite entre la divisibilité dans $\mathbb{Z}$ et l'ordre naturel dans $\mathbb{Q}$ :

**Proposition 3.3.7.** *Si $r$ est un nombre rationnel, alors la partie entière de $r$ est le quotient de la division euclidienne de $a$ par $b$, pour toute représentation de $r$ sous la forme $a/b$ avec $b > 0$.*

**Exemple 3.3.8.** Pour trouver la partie entière du nombre rationnel $r = -63/19$, effectuons la division euclidienne de 63 par 19 : on obtient $63 = 3.19 + 6$, d'où $-63 = (-3).19 - 6 = (-4).19 + 13$, donc $-4$ est le quotient de la division euclidienne de $-63$ par 19. Il s'ensuit que la partie entière de $r$ est $-4$.

## La valeur absolue dans $\mathbb{Q}$

Nous terminons l'inventaire de la "structure naturelle" de l'ensemble $\mathbb{Q}$ par l'extension de la valeur absolue, dont la définition est possible grâce à la propriété de "trichotomie" de l'ordre naturel (proposition 3.3.1).

**Définition 3.3.9.** Si $r$ est un nombre rationnel, la *valeur absolue de* $r$ est le nombre rationnel $r$ si $r \geq 0$, le nombre rationnel $-r$ si $r < 0$.

Les propriétés usuelles de la valeur absolue, introduites à la proposition 2.3.4 pour les nombres entiers relatifs, sont vérifiées :

**Proposition 3.3.10.** *Pour tous nombres rationnels $r$ et $s$, on a :*
*i)* $|r| = 0$ *si et seulement si* $r = 0$
*ii)* $|rs| = |r|.|s|$
*iii)* $|r + s| \leq |r| + |s|$ *(et égalité si $r$ et $s$ sont de même signe).*

*Démonstration.* La démonstration est identique à celle de 2.3.4.
i) Si $|r| = 0$, alors soit $r \geq 0$ et alors $r = |r| = 0$, soit $r < 0$, et alors $|r| = -r > 0$, ce qui est impossible. Le second cas est exclu, donc par le premier cas on a $r = 0$. Réciproquement, par définition on a $|0| = 0$.
ii) Distinguons plusieurs cas. Si $r = 0$ ou $s = 0$, on a $rs = 0$, donc $|rs| = |r|.|s|$ par (i). Supposons que $r, s > 0$ : on a $rs > 0$ par 3.3.2, donc $|rs| = rs = |r|.|s|$. De même, si $r, s < 0$ on a $rs > 0$ et donc $|rs| = rs = (-r).(-s) = |r|.|s|$. Enfin, si $r$ et $s$ sont non nuls et de signes contraires, par exemple $r > 0$ et $s < 0$, on a $rs < 0$, d'où $|rs| = -rs = r.(-s) = |r|.|s|$ et de même pour l'autre cas.
iii) Distinguons aussi plusieurs cas. Si $r, s \geq 0$, alors $r + s \geq 0$ par 3.3.2 à nouveau, donc $|r + s| = r + s = |r| + |s|$, d'où l'inégalité. Si $r, s < 0$, alors $r + s < 0$, donc $|r + s| = -(r + s) = -r - s = |r| + |s|$, et l'inégalité est encore vérifiée. Enfin, si par exemple $r \geq 0$ et $s < 0$, on a $r + s < r < r - s = |r| + |s|$, et on distingue à nouveau deux cas : si $r + s \geq 0$, on a $|r + s| = r + s \leq |r| + |s|$ par l'inégalité précédente, tandis que si $r + s < 0$, on a $|r + s| = -s - r \leq -s$ (puisque $-r \leq 0$), et comme $-s = |s| \leq |r| + |s|$, on a aussi $|r + s| \leq |r| + |s|$. Le cas où $r < 0$ et $s \geq 0$ se traite de la même manière. □

## Exercices de la section

*Exercice* 3.3.11. i) Démontrer l'analogue de la proposition 3.3.2 en remplaçant les inégalités strictes par des inégalités larges.
ii) Démontrer que tout carré dans $\mathbb{Q}$ est positif, autrement dit que pour tout nombre rationnel $q$, on a $q^2 \geq 0$.
iii) En utilisant des comparaisons à des entiers relatifs, comparer sans calcul les nombres rationnels $-75/23$ et $-18/7$.
iv) Comparer les nombres $1316/514$ et $734/279$.
iii) Quelle est la partie entière du nombre rationnel $1372/43$ ? Du nombre rationnel $725/-18$ ?
iv) Dessiner les différentes situations correspondant aux différents cas possibles (selon les signes de $r$ et $s$) de la clause (iii) de la proposition 3.3.10 : représenter $r, s$, $|r|$, $|s|$ et $|r + s|$.

## 3.4 Décomposition multiplicative et valuations $p$-adiques

Dans cette section et jusqu'à la fin du chapitre, nous abordons l'extension de propriétés arithmétiques de l'ensemble $\mathbb{Z}$ à l'ensemble $\mathbb{Q}$. Mais puisque en axiomatisant cet ensemble, nous avons ajouté des inverses multiplicatifs à tout élément non nul, par la proposition 3.2.9 tout nombre rationnel $q$ est divisible par tout nombre rationnel non nul $r$ ! Cela signifie que la relation de divisibilité ne présente plus aucun intérêt arithmétique dans l'ensemble $\mathbb{Q}$, or nous avons défini l'arithmétique dans $\mathbb{N}$ et dans $\mathbb{Z}$ comme l'étude de cette relation...
En fait, l'existence des décompositions en nombres premiers subsiste de manière essentielle dans la théorie des nombres rationnels, et on l'étudie en rapport à des "raffinements" associés à chaque nombre premier et obtenus à partir de l'extension de la notion d'exposant évoquée à la section 2.6.1, laquelle nécessite de définir auparavant les puissances négatives d'un nombre rationnel.

### 3.4.1 Puissances des nombres rationnels

Dans la section 2.5.1, nous avons défini proprement la puissance d'un nombre entier relatif par un entier naturel quelconque. Nous allons définir ici la puissance d'un nombre rationnel par un entier *relatif*.

**Définition 3.4.1.** Soit $r$ un nombre rationnel.
A) Si $n$ est un nombre entier *naturel*, on définit le nombre rationnel $r$ *(à la) puissance* $n$, noté $r^n$, par récurrence, de la manière suivante :
i) Si $n = 0$, on pose $r^0 = 1$
ii) On pose $r^{n+1} := r^n.r$, en supposant que $r^n$ est défini.
B) Si $r$ est non nul et $n$ est un nombre entier *négatif*, on définit le nombre rationnel $r^n$ comme $1/r^{-n}$.

La définition de la puissance d'un nombre rationnel par un entier naturel est exactement la même que celle de la puissance d'un nombre entier relatif : elle prolonge donc celle-ci et c'est celle que nous adopterons aussi pour les nombres réels et les nombres complexes.
L'extension de la définition consiste principalement à définir les puissances négatives à partir de l'inversion. Cette définition est justifiée dans la mesure où pour tout nombre rationnel $r \neq 0$ et tout entier $n \leq 0$, l'entier $-n$ est positif, et le nombre rationnel $r^{-n}$ est donc bien défini par récurrence et différent de zéro. Il faut prendre garde toutefois que la puissance n'est pas toujours définie pour $r = 0$, puisque $0^1 = 0$, et donc que $0^{-1}$ n'a pas de sens. C'est en fait le seul cas où $r^n$ ne peut pas être défini pour $n < 0$.
Les propriétés des puissances entières des nombres rationnels sont essentiellement les mêmes que dans le cas des nombres entiers (évoquées à la proposition 2.5.2) :

**Proposition 3.4.2.** *Soient $q$ et $r$ des nombres rationnels, et $m, n$ des entiers relatifs. Lorsque les puissances sont toutes définies, on a :*
*i)* $(q.r)^m = q^m.r^m$

*ii)* $q^{m+n} = q^m.q^n$
*iii)* $(q^m)^n = q^{m.n}$.

*Démonstration.* Lorsque $m, n \geq 0$, les puissances sont toujours définies et les démonstrations sont identiques à celles de la démonstration de 2.5.2 : nous ne les reproduisons pas ici. On traite donc du cas où l'un des nombres $m$ et $n$ est strictement négatif, et par symétrie on peut choisir $m < 0$.
i) On a $(q.r)^m = 1/(q.r)^{-m}$ (par définition) $= 1/(q^{-m}.r^{-m})$ (par le cas $m > 0$) $= (1/q^{-m}).(1/r^{-m}) = q^m.r^m$ (par définition).
ii) On distingue deux cas, selon que $m + n \geq 0$ ou que $m + n < 0$. Supposons que $m + n \geq 0$, posons $k = m + n$ et raisonnons par récurrence sur $k$. Si $k = 0$, on a $m = -n$, et $q^{m+n} = q^k = q^0 = 1 = (q^m).(1/q^m) = q^m.q^{-m} = q^m.q^n$ et la propriété est vérifiée. Supposons qu'elle le soit au rang $k$, et que $m + n = k + 1$ : comme $m < 0$, on a $n > 0$, donc on peut écrire $n$ sous la forme $n = l + 1$, d'où $m + l = k$, et on a alors $q^{m+n} = q^{k+1} = q^{m+l+1} = q^{m+l}.q$ (par définition) $= (q^m.q^l).q$ (par hypothèse de récurrence appliquée à $m + l = k$) $= q^m.q^{l+1} = q^m.q^n$, et la propriété est vérifiée au rang $k + 1$. Par récurrence, elle l'est pour tout $k \in \mathbb{N}$, donc pour tous $m, n$ tels que $m < 0$ et $m + n \geq 0$. Supposons maintenant que $m + n < 0$, et distinguons à nouveau deux cas, selon que $n \leq 0$ ou $n > 0$. Si $n \leq 0$, on a $q^{m+n} = 1/q^{-m-n}$ (par définition) $= 1/(q^{-m}.q^{-n})$ (par le cas $m, n \geq 0$) $= (1/q^{-m}).(1/q^{-n}) = q^m.q^n$. Si $n > 0$, on a $-n < 0$ et : comme $-m - n > 0$, par le cas $m + n \geq 0$ et en échangeant les rôles de $n$ et de $-m$, on obtient également $q^{m+n} = 1/q^{-m-n} = 1/(q^{-m}.q^{-n}) = (1/q^{-m}).(1/q^{-n}) = q^m.q^n$.
iii) On a $(q^m)^n = (1/q^{-m})^n$ (par définition d'une puissance négative) $= (1/q)^{-mn}$ (par le cas $m, n \geq 0$) $= q^{mn}$. □

Notons que par définition, si $r$ est un nombre rationnel non nul, on a $r^{-1} = 1/r$, et donc pour tout entier naturel $n$, $(1/r)^n = (r^{-1})^n = r^{-n} = 1/r^n$ par la proposition 3.4.2.

### 3.4.2 Valuations $p$-adiques

La factorisation des entiers naturels (et donc des entiers relatifs) en produit de puissances de nombres premiers (théorème 2.5.10) peut dans un certain sens s'étendre aux nombres rationnels. Il existe au moins deux façons de le faire : nous commençons par exposer la plus simple, qui consiste à décomposer le numérateur $a$ et le dénominateur $b$ d'une représentation $a/b$ d'un nombre rationnel en nombres premiers $p_1, \ldots, p_n$, et à réécrire la fraction $a/b$ sous la forme d'un produit de ces facteurs premiers, **avec des puissances positives ou négatives**.
En sélectionnant un des nombres premiers $p_i$ de cette décomposition "multiplicative", nous pouvons alors considérer le nombre $a/b$ "relativement au nombre $p_i$", ce qui permet d'en tirer des informations arithmétiques intéressantes. Or, si $p \in \mathbb{N}$ est un nombre premier, nous avons défini dans la section 2.6.1 l'exposant de $p$ dans un entier relatif non nul. Nous pouvons utilement étendre cette notion à tout nombre rationnel non nul de la manière suivante :

**Définition 3.4.3.** Si $r = a/b$ est un nombre rationnel non nul, la *valuation $p$-adique de $r$* est le nombre entier relatif $v_p(r) = v_p(a) - v_p(b)$, où $v_p(a)$ est l'exposant de $p$

dans $a$.

**Remarque 3.4.4.** La valuation ne peut être définie que pour un nombre rationnel non nul, puisque si $a = 0$, l'exposant de $p$ dans $a$ n'est pas défini.

*A priori*, la valuation $p$-adique pourrait dépendre du choix d'une représentation d'un rationnel non nul. Pour montrer qu'elle ne dépend pas d'un tel choix et qu'elle est donc bien définie, supposons que $r = a/b = c/d$ : on a $ad = bc$ dans $\mathbb{Z}$, donc par la proposition 2.6.7, $v_p(a) + v_p(d) = v_p(ad) = v_p(bc) = v_p(b) + v_p(c)$, si bien que $v_p(a) - v_p(b) = v_p(c) - v_p(d)$, et $v_p(r)$ est bien définie.
Aussi, notons que si $n \in \mathbb{Z}$, on a $v_p(n/1) = v_p(n) - v_p(1) = v_p(n)$ pour tout entier naturel premier $p$, puisque $p$ ne divise pas 1, si bien que la valuation $p$-adique d'un entier non nul $n$ vu comme le nombre rationnel $1/n$ est l'exposant de $p$ dans $n$ : les valuations $p$-adiques sont les prolongements des exposants de $\mathbb{Z}^*$ à $\mathbb{Q}^*$.
Tout comme l'exposant "transforme" la multiplication des entiers relatifs non nuls en l'addition des entiers naturels, la valuation "transforme" la multiplication des rationnels non nuls en l'addition des entiers relatifs. Cette propriété est regroupée avec les propriétés élémentaires des valuations $p$-adiques dans la proposition suivante. Toutes ces propriétés sont analogues de celles de la valeur absolue (section 3.3.2), pour des raisons profondes qui dépassent le cadre de ce cours.

**Proposition 3.4.5.** *Pour tous nombres rationnels non nuls $r$ et $s$, on a :*
*i)* $v_p(1) = 0$
*ii)* $v_p(r.s) = v_p(r) + v_p(s)$
*iii)* $v_p(r + s) \geq \min\{v_p(r), v_p(s)\}$.

*Démonstration.* i) On a $v_p(1) = v_p(1/1) = v_p(1) - v_p(1) = 0$.
ii) Ecrivons $r = a/b$ et $s = c/d$ : on a $v_p(r.s) = v_p(ac/bd) = v_p(ac) - v_p(bd)$ (par définition) $= v_p(a)+v_p(c)-v_p(b)-v_p(d)$ (par la proposition 2.6.7) $= (v_p(a)-v_p(b))+(v_p(c) - v_p(d)) = v_p(r) + v_p(s)$.
iii) Avec les mêmes notations, nous voulons montrer que $v_p(ad + bc) - v_p(bd) \geq \min\{v_p(a) - v_p(b), v_p(c) - v_p(d)\}$. En réécrivant $v_p(bd) = v_p(b) + v_p(d)$, distinguons deux cas, selon la valeur du minimum $m := \min\{v_p(a) - v_p(b), v_p(c) - v_p(d)\}$ au membre de droite de l'inégalité à démontrer. Si $m = v_p(a) - v_p(b)$, nous voulons montrer que $v_p(ad + bc) - v_p(b) - v_p(d) \geq v_p(a) - v_p(b)$, ou encore en ajoutant $v_p(b) + v_p(d)$ aux deux membres, que $v_p(ad + bc) \geq v_p(a) + v_p(d) = v_p(ad)$. Or, par définition on a $p^{v_p(ad)}|ad$ et comme $v_p(a) - v_p(b) \leq v_p(c) - v_p(d)$, on a $v_p(ad) = v_p(a) + v_p(d) \leq v_p(c) + v_p(b) = v_p(bc)$, d'où aussi $p^{v_p(ad)}|bc$, si bien que finalement, on a $p^{v_p(ad)}|ad + bc$, d'où $v_p(ad + bc) \geq v_p(a) + v_p(d)$, par définition de l'exposant de $p$ dans $ad + bc$. Si $m = v_p(c) - v_p(d)$, on raisonne exactement de la même manière en échangeant les rôles de $(a, b)$ et de $(c, d)$. □

La valuation $p$-adique d'un nombre rationnel non nul est toujours un entier relatif. Grâce à cette notion, on peut établir la décomposition multiplicative d'un nombre rationnel strictement positif comme généralisation de la décomposition d'un entier naturel en nombres premiers.

**Lemme 3.4.6.** *Soient $r$ un nombre rationnel strictement positif, et $(a, b)$ sa forme irréductible canonique. Si $p$ est un entier naturel premier, alors :*

*i) On a $v_p(r) = 0$ si et seulement $p$ ne divise ni $a$, ni $b$*
*ii) On a $v_p(r) > 0$ si et seulement si $p|a$ mais $p \nmid b$, et alors $v_p(r) = v_p(a)$*
*iii) On a $v_p(r) < 0$ si et seulement si $p|b$ mais $p \nmid a$, et alors $v_p(r) = -v_p(b)$.*

*Démonstration.* i) Par définition, on a $v_p(r) = v_p(a) - v_p(b)$, donc si $v_p(r) = 0$, on a $v_p(a) = v_p(b)$ : si $v_p(a) > 0$, alors $p|a$ et $p|b$, ce qui contredit la primalité relative de $a$ et $b$, d'où $p \nmid a$ et $p \nmid b$. Inversement, si $p$ ne divise ni $a$, ni $b$, on a $v_p(r) = v_p(a) - v_p(b) = 0 - 0 = 0$.
ii) Supposons que $v_p(r) > 0$ : si $b|p$, on a $v_p(a) > v_p(b) > 0$, donc $p|a$ également, ce qui est impossible à nouveau puisque $pgcd(a, b) = 1$. On en déduit que $p \nmid b$, $v_p(b) = 0$, et $v_p(r) = v_p(a) - v_p(b) = v_p(a)$. Inversement, si $p|a$ on ne peut avoir $p|b$ par primalité relative, donc on a $v_p(r) = v_p(a) > 0$.
iii) Supposons que $v_p(r) < 0$ : si $a|p$, on a $v_p(b) > v_p(a) > 0$, donc $p|b$ également, ce qui est impossible, d'où $p \nmid a$, $v_p(a) = 0$, et $v_p(r) = v_p(a) - v_p(b) = -v_p(b)$. La réciproque se démontre de manière évidente. □

Dans le théorème suivant, qui prolonge le théorème 2.5.10, nous utilisons une notation nouvelle pour le produit d'un nombre fini de nombres rationnels. La notation est analogue à celle des sommes finies (section 2.7.6), sauf qu'on ajoute à l'indexation (ici $i$ variant de 1 à $n$) une condition sur les indices (ici $v_{p_i}(r) > 0$ ou $v_{p_i}(r) < 0$). Ceci signifie qu'on effectue le produit des nombres indexés par $i$, en ne retenant que ceux pour lesquels la condition sur l'indice $i$ est vérifiée. En toute rigueur nous devrions définir intégralement le procédé, ce que nous ferons plutôt dans un cours ultérieur : la notation est ici suffisamment claire.

**Théorème 3.4.7.** *Si $r$ est un nombre rationnel strictement positif, il existe un entier naturel $n$ et des nombres premiers $p_1 < \ldots < p_n$ uniques, ainsi que des entiers relatifs non nuls $k_1, \ldots, k_n$ uniques, tels que $r = p_1^{k_1} \ldots p_n^{k_n}$. De plus, les nombres $k_i$ sont les $v_{p_i}(r)$.*

*Démonstration.* Si $r = 1$, alors $n = 0$ convient : la décomposition est "vide". Si $r \neq 1$, écrivons $r = a/b$ sous forme irréductible canonique, c'est-à-dire avec $b > 0$ et $a$ et $b$ premiers entre eux, de sorte que $a \neq b$. Soient $n \in \mathbb{N}$ et $p_1 < \ldots < p_n$ les nombres premiers apparaissant avec un exposant non nul soit dans la décomposition de $a$ en nombres premiers, soit dans celle de $b$. Par le lemme 3.4.6, pour tout $i = 1, \ldots, n$ on a $v_{p_i}(r) \neq 0$, et $a = \prod_{i, v_{p_i} > 0} p_i^{v_{p_i}(r)}$ et $b = \prod_{i, v_{p_i}(r) < 0} p_i^{-v_{p_i}(r)}$, d'où $r = a/b = \prod_i p_i^{v_{p_i}(r)}$, et l'existence de la décomposition est démontrée. Concernant l'unicité de la décomposition, supposons que $r = p_1^{k_1} \ldots p_n^{k_n}$ avec $p_1 < \ldots < p_n$ des entiers naturels premiers et $k_i \in \mathbb{Z}^*$ pour tout $i = 1, \ldots, n$, et soit à nouveau $(a, b)$ la forme irréductible canonique de $r$. Par le lemme 3.4.6, les nombres premiers $p_i$, $i = 1, \ldots, n$, sont les facteurs premiers de $a$ ou de $b$, et pour tout $i = 1, \ldots, n$ on a $k_i = v_{p_i}(r)$, si bien que la décomposition est unique. □

**Exemple 3.4.8.** Décomposons le nombre rationnel $r = 6375/1485$ en nombres premiers. Le numérateur et le dénominateur sont divisibles par 5, on peut donc simplifier en $r = 1275/297$. Deux décompositions en nombres premiers donnent $1275 = 3.5^2.17$ et $297 = 3^3.11$, donc la décomposition cherchée est $r = 3^{-2}.5.11^{-1}.17$.

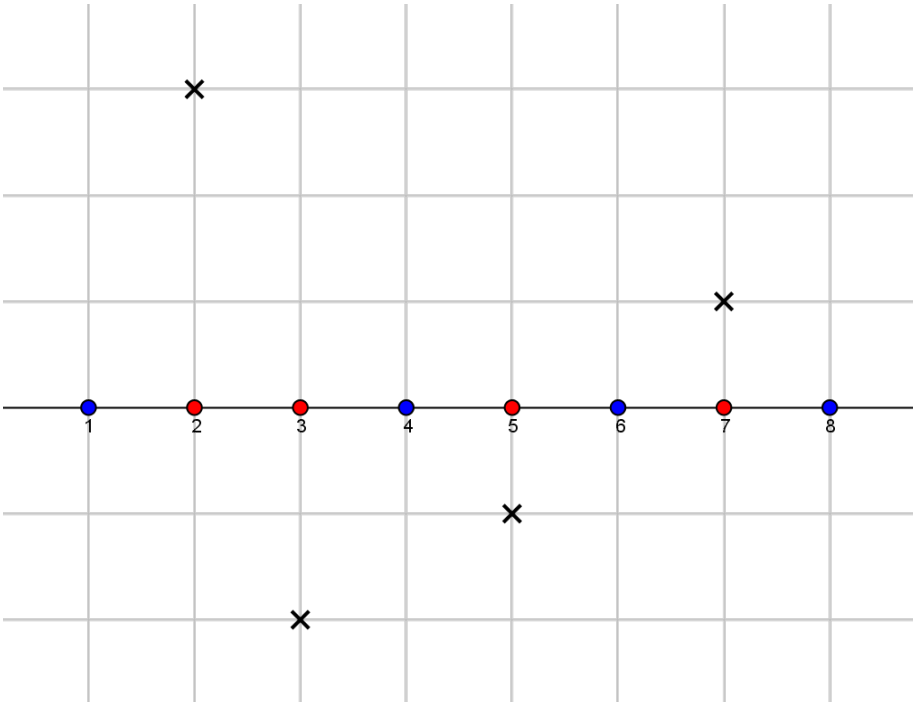



Figure 17: Le nombre rationnel 504/405 se décompose sous la forme $2^3.3^2.7/3^4.5$. Sa forme irréductible est donc $2^3.7/3^2.5 = 56/45$, d'où la représentation $2.3^{-2}.5^{-1}.7$ en produit de puissances entières relatives de nombres premiers.

La figure 17 propose une interprétation graphique de la décomposition d'un nombre rationnel positif en puissances de nombres premiers.
Grâce à la notion de valuation, on peut aussi redémontrer de manière élémentaire que le nombre réel $\sqrt{2}$ n'est pas rationnel :

**Proposition 3.4.9.** *Il n'existe aucun nombre rationnel $r$ tel que $r^2 = 2$.*

*Démonstration.* Supposons par l'absurde qu'il existe $r \in \mathbb{Q}$, nécessairement non nul, tel que $r^2 = 2$. On considère alors la valuation 2-adique de 2, qui vaut 1 puisque 1 est l'exposant de 2 dans 2. Par la proposition 3.4.5, on peut aussi écrire $v_2(r^2) = v_2(r.r) = v_2(r) + v_2(r) = 2v_2(r)$. Il s'ensuit que $1 = 2v_2(r)$, soit $v_2(r) = \frac{1}{2}$, ce qui est impossible puisque la valuation 2-adique est toujours un entier relatif. Par *reductio ad absurdum*, on en déduit qu'il n'existe pas de racine carrée de 2 dans l'ensemble $\mathbb{Q}$. □

L'élément déterminant dans la démonstration de la proposition 3.4.9 est le caractère impair de l'exposant de 2 (sa valuation 2-adique comme nombre rationnel) dans le nombre entier 2. Cette idée permet en fait de caractériser tous les nombres rationnels qui possèdent une racine carrée dans $\mathbb{Q}$.

**Théorème 3.4.10.** *Un nombre rationnel $r$ possède une racine carrée dans $\mathbb{Q}$ si et seulement si il est positif et pour tout entier naturel premier $p$, l'entier relatif $v_p(r)$ est pair.*

*Démonstration.* Si $r < 0$, alors comme le carré d'un nombre rationnel est toujours positif par 3.3.2, $r$ ne peut avoir de racine carrée; par contraposée un entier rationnel

possédant une racine carrée est toujours positif. Si $r = 0$, on a $r = 0^2$, donc $r$ possède une racine carrée. Supposons désormais que $r > 0$ et décomposons $r$ en facteurs premiers sous la forme $p_1^{v_{p_1}(r)} \dots p_n^{v_{p_n}(r)}$ par le théorème 3.4.7. Si pour tout entier naturel premier $p$, l'entier $v_p(r)$ est pair, en particulier pour $i = 1, \dots, n$ $v_{p_i}(r)$ est pair, on peut l'écrire sous la forme $v_{p_i}(r) = 2k_i$, $k_i \in \mathbb{Z}$. Le nombre rationnel $q = p_1^{k_1} \dots p_n^{k_n}$ est alors une racine carrée de $r$, puisque $q^2 = p_1^{2k_1} \dots p_n^{2k_n} = r$. Réciproquement, si $r$ possède une racine carrée rationnelle $s$, on peut supposer que $s > 0$ (car si $s < 0$, on a $-s > 0$ et $(-s)^2 = s^2 = r$, donc on peut toujours en tirer une racine carrée positive). Décomposons $s$ en facteurs premiers sous la forme $q_1^{l_1} \dots q_m^{l_m}$, avec $q_1 < \dots < q_m$ et $v_{q_j}(s) = l_j \in \mathbb{Z}^\times$ pour tout $j$ : on a $s^2 = q_1^{2l_1} \dots q_m^{2l_m} = r$, donc par unicité de la décomposition de $r$ (théorème 3.4.7) on a $\{q_1, \dots, q_m\} = \{p_1, \dots, p_n\}$ et la valuation $p_i$-adique $v_{p_i}(r) = 2l_i$ de $r$ est paire pour tout $i = 1, \dots, n$. Puisque la valuation $p$-adique de $r$ est nulle pour tous les autres entiers naturels premiers $p$ par le lemme 3.4.6, elle est paire pour tous les nombres premiers. □

## Exercices de la section

*Exercice* 3.4.11. i) Démontrer par récurrence que pour tout entier naturel premier $p$, pour tout nombre rationnel non nul $r$ et pour tout entier naturel $m$, on a $v_p(r^m) = m.v_p(r)$. En déduire que pour tout entier naturel premier $p$ et pour tout entier naturel $m > 1$, $p$ n'a pas de racine $m$-ième dans $\mathbb{Q}$ (c'est-à-dire qu'il n'existe pas de nombre rationnel $r$ tel que $r^m = p$).
ii) Soit $r$ un nombre rationnel non nul. Montrer que $v_p(r) = v_p(|r|)$ pour tout entier naturel premier $p$.
iii) Démontrer la réciproque de la clause (iii) du lemme 3.4.6.

*Problème* 3.4.12. L'objectif de ce problème est de généraliser le théorème 3.4.10 sous la forme suivante : si $m$ est un entier naturel $> 1$ et $r$ un rationnel non nul, alors $r$ possède une racine $m$-ième dans $\mathbb{Q}$ (c'est-à-dire : il existe un rationnel $s$ tel que $s^m = r$) si et seulement si on se trouve dans l'un des deux cas (mutuellement exclusifs) suivants :
- $m$ est pair, $r > 0$ et $m|v_p(r)$ pour tout nombre premier $p$
- $m$ est impair et $m|v_p(r)$ pour tout nombre premier $p$.

A) On suppose d'abord que $m$ est pair.
i) Montrer que si $r < 0$, $r$ ne possède pas de racine $m$-ième dans $\mathbb{Q}$.
ii) Montrer que si $r > 0$, alors $r$ possède une racine $m$-ième dans $\mathbb{Q}$ si et seulement si $m|v_p(r)$ pour tout nombre premier $p$.
B) On suppose désormais que $m$ est impair.
iii) Montrer que si $r \neq 0$ et $m|v_p(r)$ pour tout nombre premier $p$, et si $p_1^{k_1} \dots p_n^{k_n}$ est la décomposition de $|r|$ en facteurs premiers, alors pour $s := p_1^{k_1/m} \dots m_n^{k_1/m}$, on a $(|r|/r)^m.s^m = r$.
iv) Montrer que si $r \neq 0$ et $r$ possède une racine $m$-ième $s$ dans $\mathbb{Q}$, alors $m|v_p(r)$ pour tout nombre premier $p$.
C) Conclure, sans oublier de traiter le cas où $r = 0$.

## 3.5 Commensurabilité

Si $n$ et $m$ sont deux entiers relatifs non nuls, tout diviseur positif commun $d$ de $n$ et $m$ s'interprète géométriquement comme une "unité de mesure" commune qui permet de représenter $n$ et $m$ comme grandeurs "mesurables" par des nombres entiers dans cette unité. L'existence de mesures communes à des grandeurs géométriques était un des thèmes essentiels de la géométrie de l'école pythagoricienne.
Dans cette section nous franchissons la frontière entre l'arithmétique et la géométrie pour proposer une analyse géométrique des nombres rationnels à partir de la problématique antique de la commensurabilité, qui a abouti à la découverte de l'irrationalité (c'est-à-dire la "non-rationalité") de certaines grandeurs, la première d'entre elles étant $\sqrt{2}$.
En suivant la même philosophie que dans le reste de ce volume, nous inscrirons ce sujet dans le prolongement de l'étude des diviseurs communs des entiers relatifs, et notamment de la section 2.4 et du théorème de Bézout 2.4.3.

**Définition 3.5.1.** Nous dirons que deux nombres réels $x$ et $y$ sont *commensurables* si il existe un nombre réel $\alpha > 0$ et des entiers relatifs $u$ et $v$ tels que $x = u.\alpha$ et $y = v.\alpha$.

Autrement dit, deux nombres réels sont commensurables lorsqu'ils ont une "unité de mesure commune". Nous faisons appel pour l'instant à l'intuition des nombres réels et des leurs propriétés, évoquées dans le cours n° 1; nous décrirons l'ensemble de ces nombres de manière axiomatique au cours suivant, comme extension de l'ensemble $\mathbb{Q}$. Cette propriété se reformule aisément de la manière suivante :

**Proposition 3.5.2.** *Deux nombres réels non nuls $x$ et $y$ sont commensurables si et seulement si leur rapport $x/y$ est un nombre rationnel.*

*Démonstration.* Supposons que $x$ et $y$ soient commensurables et soient $\alpha > 0$ un nombre réel et $u, v \in \mathbb{Z}$ deux entiers non nuls tels que $x = u.\alpha$ et $y = v.\alpha$ : on a $x/y = u.\alpha/v.\alpha = u/v \in \mathbb{Q}$. Réciproquement, si $x/y \in \mathbb{Q}$, écrivons $x/y = u/v$, avec $u, v \in \mathbb{Z}$ non nuls : on a $x.v = y.u$, d'où $x = u.(y/v)$ et $y = v.(y/v)$, et le réel $\alpha = |y/v| > 0$ convient comme commune mesure de $x$ et de $y$. □

Nous avons introduit la définition 3.5.1 dans le contexte général des nombres réels, car deux tels nombres ne sont pas toujours commensurables, contrairement au cas des nombres rationnels :

**Proposition 3.5.3.** *Deux nombres rationnels non nuls quelconques sont toujours commensurables par un nombre rationnel. Autrement dit, si $r = a/b, s = c/d \in \mathbb{Q}^*$, il existe un nombre rationnel $\alpha > 0$ et $u, v \in \mathbb{Z}$ tels que $r = u\alpha$ et $s = v\alpha$. De plus, le plus grand nombre $\alpha$ ayant cette propriété est $pgcd(ad, bc)/bd$.*

*Démonstration.* Quitte à changer le signe de $u$ et/ou de $v$, on peut se ramener au cas où $r, s > 0$ : commençons donc par faire cette hypothèse, en supposant en outre que $b, d > 0$. Ecrivons $r = a/b$ et $s = c/d$, et considérons les entiers naturels non nuls $ad$ et $bc$ : si $e$ est un diviseur positif commun à $ad$ et $bc$, il existe $u, v \in \mathbb{N}$ tels que $ad = ue$ et $bc = ve$. On peut alors écrire $r = a/b = ad/bd = u.(e/bd)$, et

$s = c/d = bc/bd = v.(e/bd)$, si bien que $\alpha = e/bd$ convient. Dans le cas général, par ce qui précède on trouve un nombre rationnel $\alpha > 0$ et $u, v \in \mathbb{N}$ tels que $|r| = u'.\alpha$ et $|s| = v'.\alpha$, d'où $r = ((r/|r|).u').\alpha$ et $s = ((s/|s|).v')).\alpha$, et les entiers relatifs $u = (r/|r|).u'$ et $v = (s/|s|).v'$ conviennent.
Supposons maintenant que $\alpha = h/l > 0$ est un nombre rationnel ayant cette propriété, avec $h, l > 0$ : comme avant, nous nous ramenons au cas où $r, s > 0$, et il existe $u, v \in \mathbb{N}$ tels que $u\alpha = r$ et $v\alpha = s$. Réécrivons ceci sous la forme $uh/l = a/b$ et $vh/l = c/d$, ou encore $uhb = al$ et $vhd = cl$. En multipliant la première égalité par $d$ on obtient $adl = uhbd$ et en multipliant la seconde par $b$ on obtient $bcl = vhbd$. Soit $e = pgcd(ad, bc)$ : on a $el = pgcd(adl, bcl)$ par la proposition 2.4.8(ii), si bien que $hbd$ divise $el$, puisqu'il divise $adl$ et $bcl$. On en déduit que $hbd \leq el$, puisque tous ces nombres sont positifs, si bien que $\alpha = h/l = hbd/lbd \leq el/lbd = e/bd$, et la proposition est démontrée, puisque $\alpha = e/bd$ convient également, par la première partie de la démonstration. □

**Remarque 3.5.4.** Un nombre rationnel $\alpha > 0$ ayant les propriétés de l'énoncé est une *commune mesure (rationnelle) de $r$ et $s$*. Par la seconde partie de la proposition, il en existe toujours une plus grande.

**Exemple 3.5.5.** Trouvons une commune mesure (la plus grande), entre les nombres rationnels $26/15$ et $-156/47$, en calculant le p.g.c.d de $26.47$ et $15.156$. On a $26 = 2.13$, $15 = 3.5$ et $156 = 2^2.3.13$, tandis que $47$ est premier : on a donc $pgcd(26.47, 15.156) = 2.13 = 26$, si bien que la plus grande commune mesure cherchée est $\alpha = 26/705$. En général, pour trouver la plus grande commune mesure de $a/b$ et $c/d$, on peut aussi chercher une relation de Bézout entre $ad$ et $bc$.

Comme indiqué au début de la section, la commensurabilité des nombres rationnels et la primalité relative des entiers relatifs sont fondamentalement liées, à travers la notion de plus grand commun diviseur, et de la manière suivante.
Si $a$ et $b$ sont deux entiers relatifs non nuls et $d \in \mathbb{N}^*$ est un diviseur commun de $a$ et $b$, alors il existe $u, v \in \mathbb{Z}$ tels que $a = ud$ et $b = vd$ : en considérant $a, b$ et $d$ comme nombres rationnels, $d$ est alors une commune mesure de $a$ et $b$ au sens de 3.5.3. De plus, la plus grande commune mesure de $a$ et $b$ est donnée par $pgcd(a, b)$, puisqu'on identifie $a$ avec $a/1$ et $b$ avec $b/1$ : la formule de la proposition nous donne bien $\alpha = \frac{pgcd(a.1, b.1)}{1.1}$, qui est la représentation rationnelle de l'entier $pgcd(a, b)$.
Nous avons ainsi établi la première partie de la proposition 3.5.7, que nous démontrerons à l'aide du lemme suivant :

**Lemme 3.5.6.** *Soient $r$ un nombre rationnel et $a/b$ une forme irréductible de $r$. Pour tout entier relatif $c$, le nombre $r$ est de la forme $c/d$ si et seulement si $a$ divise $c$.*

*Démonstration.* Supposons que $a$ divise $c$ : il existe $e \in \mathbb{Z}$ tel que $c = ae$, d'où $r = a/b = ae/be = c/d$, avec $d = ae$. Réciproquement, supposons que $r = a/b = c/d$, de sorte que $ad = bc$ : comme la représentation $a/b$ est irréductible, $a$ et $b$ sont premiers entre eux, et par le lemme de Gauss 2.4.10 on a donc $a|c$. □

**Proposition 3.5.7.** *Si $a$ et $b$ sont deux entiers relatifs non nuls, les diviseurs communs de $a$ et $b$ dans $\mathbb{N}^*$ sont des mesures communes de $a$ et $b$ dans $\mathbb{Q}$, et la plus*

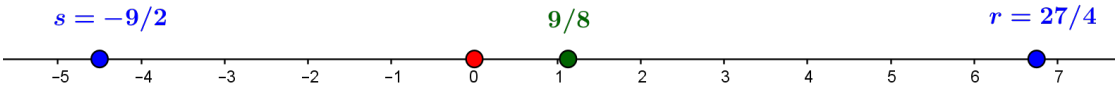



Figure 18: Le nombre rationnel positif $9/8$ est une commune mesure des nombres rationnels $r = 27/4$ et $s = -9/2$, puisque $r = 6 \times (9/8)$ et $s = (-4) \times (9/8)$. Leur plus grande commune mesure est le nombre rationnel $pgcd(27.2, 9.4)/4.2 = 9/4$.

*grande commune mesure de $a$ et $b$ est leur plus grand commun diviseur. De plus, toute mesure commune de $a$ et $b$ est de la forme $pgcd(a, b)/c$ pour $c \in \mathbb{N}^*$.*

*Démonstration.* Seule la dernière partie reste à démontrer. Soit donc $\alpha > 0$ une mesure commune de $a$ et $b$, et soit $m/n$ la forme irréductible canonique de $\alpha$. Par définition, il existe $u, v \in \mathbb{Z}$ tels que $a = u\alpha = um/n$ et $b = v\alpha = vm/n$, soit $an = um$ et $bn = vm$. Comme $m$ et $n$ sont premiers entre eux, par le lemme de Gauss 2.4.10 on a $m|a$ et $m|b$, d'où $m|pgcd(a, b)$. Par le lemme 3.5.6, il existe $c \in \mathbb{Z}$ tel que $\alpha = m/n = pgcd(a, b)/c$, et comme $\alpha, pgcd(a, b) > 0$ on a aussi $c > 0$. □

La figure 18 illustre l'existence d'une commune mesure à deux nombres rationnels. Inversement, on peut interpréter la commensurabilité comme une généralisation des relations de Bézout. En effet, si $\alpha \in \mathbb{Q}_+^*$ est la plus grande commune mesure des rationnels non nuls $r = a/b$ et $s = c/d$, écrivons une relation de Bézout entre $ad$ et $bc$ : il existe $u, v \in \mathbb{Z}$ tels que $u(ad)+v(bc) = pgcd(ad, bc)$. Puisqu'on a $r = a/b = ad/bd$ et $s = c/d = bc/bd$, on en tire $pgcd(ad, bc)/bd = uad/bd + vbc/bd = ur + vs$, si bien que nous avons démontré la propriété suivante :

**Proposition 3.5.8.** *Si $r$ et $s$ sont deux nombres rationnels non nuls et $\alpha \in \mathbb{Q}_+^*$ est leur plus grande commune mesure, alors il existe $u, v \in \mathbb{Z}$ tels que $ur + vs = \alpha$.*

De cette proposition, on peut tirer un analogue du corollaire 2.4.6 du théorème de Bézout, sous la forme suivante :

**Corollaire 3.5.9.** *Si $r$ et $s$ sont deux nombres rationnels non nuls et $\alpha \in \mathbb{Q}_+^*$ est la plus grande commune mesure de $r$ et $s$, et si $q$ est un nombre rationnel quelconque, alors il existe une solution $(u, v) \in \mathbb{Z}^2$ à l'équation $rx + sy = q$ si et seulement si $q$ est un multiple entier de $\alpha$ (c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que $q = k\alpha$).*

*Démonstration.* Supposons qu'il existe $k \in \mathbb{Z}$ tel que $q = k\alpha$ : par la proposition 3.5.8 il existe $u, v \in \mathbb{Z}$ tels que $ru+sv = \alpha$, d'où $r(uk)+s(vk) = k\alpha = q$, et $(uk, vk)$ est une solution de l'équation. Inversement, si $(u, v)$ est une solution de l'équation, de sorte que $ur+vs = q$, écrivons $r = a/b$, $s = c/d$ et $q = x/y$ sous forme irréductible canonique. On a $ua/b + vc/d = x/y$, d'où en multipliant les deux membres par $ybd$, $u.(yad) + v.(ybc) = x.(bd)$. Par le corollaire 2.4.6, on en déduit qu'il existe $k \in \mathbb{Z}$ tel que $xbd = k((yad) \wedge (ybc)) = ky.((ad) \wedge (bc))$, la dernière égalité provenant de la proposition 2.4.8 puisque $y > 0$. On peut alors écrire, par la proposition 3.5.3, $q = x/y = xbd/ybd = k.\dfrac{(ad) \wedge (bc)}{bd} = k.\alpha$, et le corollaire est démontré. □

Dans l'Antiquité, la recherche du plus grand commun diviseur de nombres entiers, ou de la plus grande commune mesure de grandeurs rationnelles, était un procédé

algorithmique connu sous le nom d'*antyphérèse*, comme le rapportent les Eléments d'Euclide. C'est la raison pour laquelle on parle d'*algorithme d'Euclide* pour la recherche du p.g.c.d.
Dans le cours n° 1, nous avons démontré dans le dernier chapitre qu'il n'existe pas de nombre rationnel $r$ tel que $r^2 = 2$, ce que nous avons redémontré ici dans la proposition 3.4.9 à l'aide des valuations. On peut interpréter ce résultat en termes "d'incommensurabilité" : par le théorème de Pythagore (que nous aborderons au cours suivant), la longueur de la diagonale d'un carré de côté 1 tracé dans le plan euclidien devrait être une grandeur strictement positive, qu'on note $\sqrt{2} > 0$, et telle que $(\sqrt{2})^2 = 2$.
Les deux longueurs (celle du côté et celle de la diagonale), c'est-à-dire 1 et $\sqrt{2}$, sont incommensurables : sinon, il existerait un nombre réel $\alpha > 0$ et des entiers $u, v$ tels que $1 = u.\alpha$ et $\sqrt{2} = v.\alpha$, d'où $\alpha = 1/u$ et $\sqrt{2} = v.(1/u) = v/u \in \mathbb{Q}$, ce qui est impossible.
L'incommensurabilité de la longueur du côté d'un carré et de la longueur de sa diagonale aurait en fait été remarquée par un mathématicien de l'école pythagoricienne, Hippase de Métaponte, et cette découverte était une tragédie pour la philosophie pythagoricienne. En effet, selon celle-ci l'harmonie de la nature se manifestait, sur le modèle des intervalles musicaux, dans tous les rapports de grandeurs, qui devaient être des nombres rationnels.
Cette découverte montre les limites essentielles de la géométrie construite à partir des nombres rationnels, ce qui motive la définition des nombres réels, que nous aborderons dans le cours n° 4, lesquels permettent de donner une représentation moderne, rigoureuse et complète, de la géométrie euclidienne du plan.

## Exercices de la section

*Exercice* 3.5.10. i) Trouver la plus grande commune mesure des nombres rationnels $-4024/1078$ et $-1521/2541$.
ii) Montrer que $5/3$ est une comme mesure des entiers 560 et 403. En déduire que ces entiers ne sont pas premiers entre eux.