TP LATEX

Naïm ZAIRI, Lucas LESAGE et Maurin GILLES

Janvier 2022

Table des matières

Première partie
L'arithmétique

1 L'ensemble des entiers naturels

1.1 Notation

Comme leur nom l'indique, les entiers dits "naturels" correspondent aux nombres tels qu'on se les représente de manière naturelle. Concrètement, ce sont ceux qui nous permettent de compter dans la vie de tous les jours.

D'un point de vue mathématique, on peut définir les entiers naturels comme les nombres strictement positifs qui peuvent s'écrire sans virgule.

L'infinité de cet ensemble est intuitive. En effet, en partant de 0, et en comptant de 1 en 1, il apparait évident qu'on pourra toujours rajouter 1, et que le comptage n'aura jamais de fin.

L'infinité de l'ensemble nous oblige donc à avoir recours à une notation spéciale pour le désigner. La notation que nous utilisons encore aujourd'hui nous vient de *Richard Dedekind*[1]. Il s'agit d'un N capital, stylisé de la manière suivante : $\mathbb{N}$

1.2 Quelques propriétés intéressantes

1.2.1 Comparaison avec les autres ensembles usuels

De par sa définition, l'ensemble $\mathbb{N}$ est le plus évident, mais donc aussi le plus basique des ensembles. Quand les mathématiques se sont complexifiées, d'autres ensembles ont été définis.

L'ensemble des entiers relatifs, noté $\mathbb{Z}$, comprend l'ensemble $\mathbb{N}$, auquel s'ajoutent tous les entiers négatifs.

L'ensemble des décimaux, noté $\mathbb{D}$, comprend tous les nombres pouvant s'écrire sous la forme $\frac{a}{10^b}$, avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}$. Concrètement, on retrouve l'ensemble $\mathbb{Z}$ pour $b = 0$.

L'ensemble des rationnels, noté $\mathbb{Q}$, comprend tous les nombres pouvant s'écrire sous la forme d'une fraction. Autrement dit, il s'agit de tous les nombres qui s'écrivent sous la forme $\frac{a}{b}$, avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}$.

L'ensemble des réels, noté $\mathbb{R}$, comprend l'ensemble des nombres qui peuvent s'écrire avec simplement une partie entière et une liste, potentiellement infinie, de décimales. Cela comprend l'ensemble $\mathbb{Q}$, ainsi que des nombres tels que e ou π.

Comme nous avons pu le voir, ces ensembles peuvent être vus comme plus ou moins grands, dans la mesure ou certains ensembles sont strictement compris dans d'autres.

En notation mathématique, on peut écrire : $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R}$

On peut aussi se représenter les choses de façon plus visuelle avec un schéma de ce type (voir figure 1).

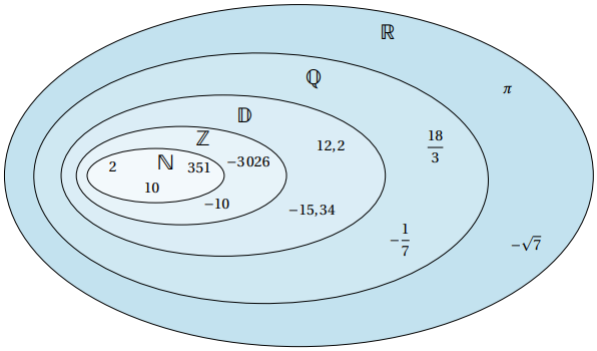

FIGURE 1 – Schéma Ensembles

(Note : si l'on s'aventure du côté des structures algébrique, on peut remarquer que l'ensemble $\mathbb{N}$ est le seul ensemble des cinq à ne pas être un groupe[2])

1.2.2 Infinis dénombrables

Par son aspect intuitif pour compter, on utilise souvent l'ensemble $\mathbb{N}$ pour étudier la cardinalité d'un autre ensemble.

Définition 1.2.2.1. ***Cardinalité :***
La cardinalité d'un ensemble E, notée $card(E)$, correspond au nombre d'éléments de E.

Corollaire 1.2.2.1. ***Ensembles finis*** *:*
E est un ensemble fini si et seulement si $card(E) \in \mathbb{N}$.

Plus rigoureusement, dire que $card(E) = n$ veut dire que l'on peut faire une bijection[3] entre l'ensemble E et l'ensemble $\{1, \ldots, n\} \subset \mathbb{N}$.

Maintenant que nous avons traité le cas des ensembles finis, regardons quand ces ensembles sont infinis :

Premièrement, on remarque que l'infini peut contenir l'infini... et peut aussi être contenu dans un autre infini ! ($2\mathbb{N} \subset \mathbb{N} \subset \mathbb{Z}$)
Compliqué de dégager une cardinalité précise de tout ça...
Mais de ce problème s'ensuit une définition fondamentale sur la cardinalité :

Définition 1.2.2.2. ***Infinis dénombrables*** *:*
Soit E un enemble infini. S'il existe une bijection entre E et $\mathbb{N}$, alors on dit que E est un ensemble dénombrable. On note sa cardinalité par ce signe :

$$Card(\mathbb{N}) = \aleph_0$$

Maintenant, avec cette définition, nous avons une réponse pour les cardinalités infinies.
Regardons lesquels des ensembles usuels sont dénombrables :

Théorème 1.2.2.1. ***Cardinalités des ensembles usuels*** *:*

$$Card(\mathbb{N}) = Card(\mathbb{Z}) = Card(\mathbb{D}) = Card(\mathbb{Q})$$

Démonstration. La démonstration étant longue et hors-sujet, elle est donc libre à vous de la trouver par vous même ou d'aller chercher la réponse sur internet ! □

Aussi fou que cela puisse paraître, même des ensembles qui paraissent intuitivement bien plus grands possèdent finalement la même cardinalité que $\mathbb{N}$.
Mais dans le théorème 1.2.2.1, on voit que l'ensemble des Réels manque à l'appel !

Théorème 1.2.2.2. ***Infinis indénombrables*** *:*
Il n'existe aucune bijection entre l'ensemble $\mathbb{N}$ et l'ensemble $\mathbb{R}$.

Par conséquent,

$$\begin{aligned} Card(\mathbb{R}) &\neq \aleph_0 \\ &= c \ (\textit{"continu"}) \end{aligned}$$

Par définition :

$$2^{\aleph_0} = c$$

Démonstration. Voir la diagonale de G. Cantor [4]. □

Et bien finalement si, certains ensembles infinis sont vraiment plus grands que... l'infini.

Une autre question se pose donc : combien y a-t-il d'infinis ?
Et bien pour l'instant nous n'avons pas encore de réponse. La possible existence d'un cardinal compris entre $\aleph^0$ et $\aleph^1$ s'appelle *"L'hypothèse du continu"*[5].

Conclusion : cet ensemble des plus simples est un puissant outil dans l'analyse des cardinaux.

2 L'arithmétique de Peano

2.1 Introduction à l'arithmétique

À l'époque de la Grèce Antique, les nombres en mathématique ne se limitaient qu'aux entiers naturels.
En effet, même les nombres décimaux étaient représentés sous forme d'entier en changeant la base.
Par exemple : si une longueur géométrique mesurait $1,9m$ alors à la place on disait que la longueur mesurait $19dm$ et on adaptait ainsi toutes les autres mesures.

(Anecdote : c'est par cette logique qu'un Pythagoricien a démontré l'existence de nombres irrationnels, des nombres ne pouvant pas être ramenés à une base car possédant une infinité de chiffres derrière la virgule !)

Par conséquent, les opérations élementaires de l'arithmétique étaient l'addition, la soustraction, la multiplication et la division.

Alors que l'addition et la multiplication sont des opérations triviales conservant la qualité d'entier d'un nombre, pour la division c'est une autre paire de manche (concernant la soustraction, l'introduction des entiers relatifs réglera ce problème).
La division classique était appelée à l'époque "Division Euclidienne".
Créée par le mathématicien Grec *Euclide*[6], cette division, bien que réadaptée au fil du temps pour s'appliquer aux entiers relatifs, permettait de ne pas avoir de partie fractionelle car il définissait une division comme étant un quotient et un reste.

Théorème 2.1.0.1. ***Division Euclidienne*** *(Version adaptée) :*
Soient $a \in \mathbb{Z}$ *et* $b \in \mathbb{N}$*, alors* $\exists!(q, r) \in \mathbb{Z} \times \mathbb{N}$ *avec* $0 \leq r < b$ *tels que :*

$$a = bq + r$$

(Note : la démonstration étant assez longue et hors-sujet, nous vous laissons voir la référence [7])

Cette définition de la division euclidienne peut sembler quelque peu abrupte, mais en fait cela est équivalent à la division euclidienne que l'on faisait en primaire ! (voir figure 2)

a := Dividende / b := Diviseur / q := Quotient / r := Reste

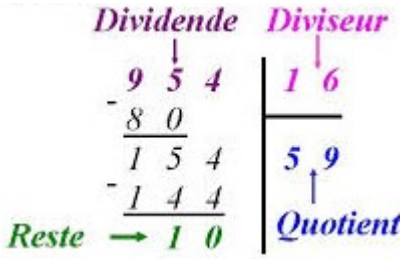

FIGURE 2 – Division euclidienne

Au cours du temps l'arithmétique n'a fait que se complexifier et se mélanger avec d'autres disciplines et créer d'autres types d'arithmétiques :

- l'arithmétique modulaire [8]

- la théorie algébrique des nombres [9]
- l'arithmétique des polynômes [10]

Mais, pendant la crise des fondements[11], le mathématicien italien *Giuseppe Peano*[12] décida en 1889 de formaliser l'arithmétique en créant un système axiomatique que l'on appela "l'arithmétique de Peano".
C'est le début des fondations de l'arithmétique moderne, mais, avant de s'atteler à cette arithmétique, nous devons d'abord introduire les symboles de la logique mathématique.

2.2 Introduction aux symboles

Un théorème de l'arithmétique de Peano est forcément écrit par ces symboles :

Opérateurs et inconnues :
Les 2 opérateurs : $+$ $\times$
Des lettres, que ce soit, latines, grecques, parfois avec des indexations, majuscules ou minuscules : x, y, δ, x_n ...

Quantificateurs : Les 2 uniques quantificateurs et leur variation :
$\forall$: Pour tout / Quel que soit
$\exists$: Il existe
$\exists!$: Il existe un unique

symboles logiques : Les symboles de la logique classique :
$\Longrightarrow$: implication
$\Longleftrightarrow$: équivalence
$\wedge$: et
$\vee$: ou
$\neg$: négation
$=$: égalité
$P(x, \ldots, x_n)$: Une propriété dépendant de n variables

symboles de Peano : Alors que les opérateurs, les quantificateurs et les symboles logiques peuvent être trouvés dans d'autres théories, les 2 prochains symboles sont propres à l'arithmétique de Peano :

1) la constante 0 : seul chiffre pouvant être écrit car son existence est assumée par l'ensemble axiomatique de Peano (nous traiterons plus profondément de ce sujet dans la section 2.3.2).

2)La fonction S (Successeur).
On pourrait intuitivement la définir comme :

$$\begin{aligned} S : \mathbb{N} &\rightarrow \mathbb{N} \\ n &\mapsto n+1 \end{aligned}$$

(Note : il faut bien comprendre qu'ici la fonction est une idée, il ne faut pas l'imaginer dans le sens d'une fonction à proprement parler. Nous l'avons mise sous cette forme pour aider à l'intuition mais à ce stade de la théorie, une fonction n'est même pas définie, c'est donc un non-sens de définir un axiome sur quelque chose qui n'existe pas.)

2.3 Les axiomes de l'arithmétique de Peano

2.3.1 Définition d'un axiome et d'un système axiomatique

Avant de se lancer à bras le corps dans le système axiomatique de Peano, il est important d'avoir une compréhension complète de ce que sont un axiome et un système axiomatique.

Définition 2.3.1.1. ***Axiome*** *[13] :*
Proposition considérée comme évidente, admise sans démonstration.

Définition 2.3.1.2. ***Système axiomatique*** *[14] :*
Ensemble d'axiomes dont certains ou tous les axiomes peuvent être utilisés logiquement pour dériver des théorèmes.

Analysons plus en détail leur signification :
Premièrement, avant de comprendre la définition, il est important de comprendre la motivation d'une telle définition.

Si l'on devait faire une analogie, l'ensemble des théories mathématiques équivaudrait à un arbre. Chaque branche est un théorème et chaque feuille ou branche liée à cette dernière est un corrolaire ou un nouveau théorème.
En effet, chaque théorème utilise des informations issues d'un autre théorème prouvé préalablement (et parfois même pas prouvé d'ailleurs... !) et ainsi de suite.
Par conséquent, les axiomes sont les racines de cet arbre, les "théorèmes originaux".
C'est pourquoi, d'après la définition 2.3.1.1, les axiomes sont des propositions, car s'il existait une démonstration, ils seraient des théorèmes et non des axiomes.

Ainsi, avec plusieurs axiomes on forme un système axiomatique, et c'est en combinant ces axiomes de manière logique qu'on peut ainsi créer des théorèmes, et ainsi de suite.
Un système axiomatique est la base d'une théorie (exemple : la théorie des ensembles ZFC ([15]) ou l'arithmétique de Peano). Ils diffèrent selon les théories, qui sont parfois plus ou moins complètes (on les appelle des théories de premier ordre ([16]) par exemple).
Le plus important pour une théorie est que'elle soit cohérente (même si on ne peut pas prouver qu'elle l'est ou non ([17]) !).

Définition 2.3.1.3. ***cohérence*** *:*
La cohérence est la propriété d'une théorie exempte de contradiction.

Plus intuitivement, un système axiomatique est dit incohérent s'il est possible de former 2 théorèmes qui prouvent quelque chose et son contraire.
Pour bien comprendre le principe d'un système axiomatique, regardons un petit exemple :

Exemple 2.3.1.1. *Créons une théorie :*
Axiome 1 : les mammifères ne pondent pas des œufs.
Axiome 2 : les ornithorynques sont des mammifères.
Axiome 3 : les ornithorynques pondent des œufs.

Nous venons de créer un système axiomatique avec ces 3 axiomes, regardons les théorèmes que l'on peut faire avec :

Théorème : les ornythorinques ne sont pas des mammifères (axiome 1+3).

Une contradiction ! ! Nous venons de créer un théorème qui contredit notre axiome 2. Par conséquent notre théorie est incohérente et n'est donc pas valide.

Maintenant que nous avons mis au clair une définition précise des axiomes et des systèmes d'axiomatiques, rentrons dans le cœur du sujet.

2.3.2 Le système axiomatique de l'arithmétique de Peano

L'arithmétique de Peano repose entièrement sur ces 5 axiomes :

1. L'élément appelé *zéro* et noté 0 est un entier naturel.
2. Tout entier naturel n a un unique successeur, noté $s(n)$ ou Sn qui est un entier naturel.
3. Aucun entier naturel n'a 0 pour successeur.
4. Deux entiers naturels ayant le même successeur sont égaux.
5. Si un ensemble d'entiers naturels contient 0 et contient le successeur de chacun de ses éléments, alors cet ensemble est $\mathbb{N}$ (on appelle plus communément cette propriété "la récurrence").

Il est important de comprendre que ces 5 axiomes ne définissent non pas l'arithmétique de Peano, mais l'ensemble des entiers naturels $\mathbb{N}$.

De manière plus intuitive, cette définition axiomatique définit $\mathbb{N}$ comme un ensemble :
1) Non-vide (car il contient l'élément 0).
2) Infini (car chaque élément possède un successeur).
3) Comprenant des entiers uniquement positifs (car pour que 0 soit le successeur d'un nombre n alors il faudrait, par définition de $S(n)$, que $n = -1$).
4) Ordonné (chaque élément ayant un unique successeur et inversement, on peut ainsi comparer les entiers entre eux, exemple : $3 < 4$).

(Note : le $5^{\text{ème}}$ axiome pose la définition que cet ensemble est bien équivalent à l'ensemble $\mathbb{N}$)

Maintenant que les bases de l'ensemble $\mathbb{N}$ ont été posées et que nous avons introduit les symboles de la logique, introduisons les 8 axiomes du système axiomatique de l'arithmétique de Peano :

1. $\forall x\ \neg(S(x) = 0)$
   (Il n'existe aucun élément x tel que son successeur est égal à 0)

2. $\forall x\ (x = 0 \vee \exists y(x = S(y)))$
   (Quel que soit l'élément x, soit il est égal à 0, soit il est le successeur d'un autre élément)

3. $\forall x \forall y\ (S(x) = S(y) \implies x = y)$
   (Si 2 éléments ont le même successeur alors ils sont égaux)

4. $\forall x\ (x + 0 = x)$
   (0 est l'élement neutre de l'addition)

5. $\forall x \forall y\ (x + S(y) = S(x + y))$
   (Se traduit intuitivement : $x + (y + 1) = (x + y) + 1$)

6. $\forall x\ (x \times 0 = 0)$
   (0 est l'élement absorbant de la multiplication)

7. $\forall x \forall y\ (x \times S(y) = (x \times y) + x)$
   (Se traduit intuitivement : $x \times (y + 1) = (x \times y) + x$, par distributivité)

8. $\forall F(x, x_1, \ldots, x_n), \forall x_1 \ldots \forall x_n$:
   $((F(0, x_1, \ldots, x_n) \wedge (\forall x(F(x, x_1, \ldots, x_n) \implies F(S(x), x_1, \ldots, x_n))))$
   $\implies \forall x F(x, x_1, \ldots, x_n)$

Bon, vous n'avez peut-être rien compris à l'axiome 8... et c'est bien normal ! Le coup de génie de Peano ici est de, même avec un langage simple, généraliser la récurrence à n'importe quel type d'affirmation (ici appélée F). Disséquons cet axiome :

Premièrement, enlevons tout les $x_1, \ldots, x_n$. On obtient donc,

$$(F(0) \wedge (\forall x(F(x) \implies F(S(x)))) \implies \forall x F(x)$$

Sous cette forme on peut reconnaître le principe de récurrence, si on traduisait l'expression littéralement on aurait :

Si une affirmation est vraie pour 0*, et si le fait qu'elle soit vraie pour* x *implique qu'elle soit vraie pour* $x + 1$*, alors l'affirmation est vraie pour tout élément* $x \in \mathbb{N}$*.*

Maintenant que nous avons compris la structure de l'axiome, il est temps de le généraliser.
En rajoutant tous ces $x_1, \ldots, x_n$, alors on généralise une affirmation à n'importe quelle affirmation existante.
Peu importe l'affirmation F et peu importe le nombre de paramètres de cette fonction, tant qu'elle possède une notion d'hérédité sur un de ses éléments alors il y a récurrence.

2.4 Conclusion

L'arithmétique est une discipline millénaire, originellement due à nos connaissances des nombres limitée, mais finalement élargie et complexifiée par le temps, devenant un outil très utilisé en cryptographie, par exemple.
C'est aussi à la fois une discipline très ardue et souvent très abstraite. Cela nous fait comprendre que la base même des nombres, les plus simples, les plus intuitifs, renferment énormément de secrets et de connaissances qu'il nous tarde de découvrir.

"La mathématique est la reine des sciences et l'arithmétique est la reine des mathématiques"

-C. F. Gauss

Deuxième partie

Les nombres premiers

1 Définition et histoire

Définition 1.0.0.1. *Un entier n supérieur ou égal à deux est dit premier si et seulement si ses seuls diviseurs positifs sont 1 et lui-même.*

Théorème 1.0.0.1. *Il y a une infinité de nombres premiers.*

Démonstration. Nous allons maintenant démontrer par l'absurde qu'il existe une infinité de nombres premiers.
Supposons que P soit fini, de cardinal n. Soient $p_1, ..., p_n$ ses éléments.
Posons $N = 1 + p_1...p_n$. On a $N \geq 2$, donc N possède un diviseur premier p (d'apres [18]).
L'entier p divise $p_1...p_n$, d'où l'on déduit que p divise 1. Cela conduit à une contradiction. P est donc infini. □

Histoire 1.0.0.1. *[19] On peut retrouver des traces des nombres premier à 20 000 ans avant notre ère, sur l'os d'Ishango où figurent les nombres 11, 13, 17 et 19.*
Durant l'antiquité, Euclide met en place des théories et des affirmations dans les "Eléments", ainsi que la décomposition en facteurs premiers. Puis, ce sera Eratosthène de Cyrène qui donnera une méthode simple pour déterminer les nombres premiers.
Par la suite, au Moyen-Age, ce sera Fibonnacci qui en fera une liste et en déterminera des critères de divisibilité. Ce sera un ecclésiastique français du nom de Marin Mersenne qui posa la question : si p est premier est-ce que $2^p - 1$ est premier ? Il a été montré que non, cependant la méthode est encore utilisée pour déterminer les nombres premiers dits "géants".
Ce sera ensuite durant la Renaissance que Goldbach affirmera que tout nombre peut s'écrire sous forme d'une somme de deux nombres premiers. Euler quant à lui prouvera que $2^{31}-1$ est premier. Gauss et Legendre vont par la suite s'intéresser à la repartition des nombres premier, montrant que plus les nombres sont dits "géants", moins les nombres premiers seront présents.
Aujourd'hui, le plus grand nombre premier connu a été decouvert en 2018 et est : $2^{82\ 589\ 933} - 1$.

2 Le théorème fondamental de l'arithmétique

Concernant les nombres premiers, les deux théorèmes à la fois les plus importants et les plus anciens, sont :
-Il y a une infinité de nombres premiers (Théorème 1.0.0.1).
-Le théorème fondamental de l'arithmétique.

Théorème 2.0.0.1. ***Théorème fondamental de l'arithmétique*** *:*
Tout entier $n > 0$ peut être écrit comme un produit de nombres premiers, de façon unique.

De ce théorème s'ensuivent un corollaire et une définition :

Corollaire 2.0.0.1. ***Nombres premiers*** *:*
Un nombre est premier si et seulement si il est l'unique facteur de sa décomposition.

Définition 2.0.0.1. ***Nombres composés*** *:*
Un entier $n > 0$ est dit composé si et seulement si il est le produit d'au moins 2 nombres.

Regardons quelques exemples pour bien comprendre comment marche une décomposition :

Exemple 2.0.0.1. *:*
- $6\ 936 = 2^3 \times 3 \times 17^2$
- $1\ 200 = 2^4 \times 3 \times 5^2$
- $7 = 7$

Les deux premiers nombres sont donc des nombres composés tandis que le dernier nombre est premier.

(La manière dont on trouve ces décompositions sera vue plus en profondeur dans les sections 3.1.1 et 4)

2.1 démonstration

Pour démontrer le Théorème fondamental de l'arithmétique, il est nécessaire de le diviser en 2 parties.
En effet, le théorème affirme l'existence d'une décomposition ; et l'unicité de cette dernière.
Il nous faudra donc prouver son existence, et ensuite prouver que cette décomposition est unique.
(La démonstration est issue d'une vidéo youtube [20])

2.1.1 Partie 1 : existence de la décomposition

Démonstration. Nous ferons une démonstration par l'absurde :
Supposons qu'il existe au moins un entier naturel qui ne possède **pas** une telle décomposition.
On pose m, le plus petit de ces entiers.
On observe que m est forcément composé (sinon il serait premier et, par définition, serait sa propre décomposition).

On pose donc,

$$m = ab \quad \text{avec } 1 < a, b < m$$

Vu que $a, b < m$, on peut écrire a et b dans leur décomposition (car on a posé m comme étant **le plus petit** entier qui ne peut pas s'écrire sous cette forme).
Donc :

$$\begin{aligned} a &= p_1^{\alpha_1} \dots p_n^{\alpha_n} \quad p_i \textit{ premiers } / \ \alpha_i \in \mathbb{N} \ \ (1 \leq i \leq n) \\ b &= q_1^{\beta_1} \dots q_m^{\beta_m} \quad q_i \textit{ premiers } / \ \beta_i \in \mathbb{N} \ \ (1 \leq i \leq m) \end{aligned}$$

mais par définition de m, on a :

$$\begin{aligned} m &= ab \\ &= p_1^{\alpha_1} \dots p_n^{\alpha_n} \times q_1^{\beta_1} \dots q_m^{\beta_m} \end{aligned}$$

m possède donc une décomposition en facteurs premiers, ce qui contredit le prédicat.
Par conséquent, on conclut qu'il n'existe pas d'entier naturel m qui ne possède pas de décomposition en facteurs premiers. □

2.1.2 Partie 2 : unicité de la décomposition

Avant de s'attaquer à l'unicité, nous devons d'abord introduire le lemme d'Euclide :

Lemme 2.1.2.1. ***Lemme d'Euclide*** *:*
Soient $b, c \in \mathbb{N}$.
*Si un nombre premier p divise le produit $b \times c$, alors p divise b **ou** p divise c.*

Démonstration. Voir la référence [21]. □

Maintenant que cela a été posé, commençons la démonstration de l'unicité de la décomposition en facteurs premiers :

Démonstration. Nous ferons aussi une démonstration par l'absurde :
Supposons que 2 décompositions différentes sont égales :

$$p_1^{\alpha_1} \dots p_n^{\alpha_n} = q_1^{\beta_1} \dots q_m^{\beta_m}$$

Nous avons 3 objectifs :
1) Montrer que $n = m$.
2) Montrer que $p_i = q_i \ \ (\forall i,\ 1 \leq i \leq n, m)$.
3) Montrer que $\alpha_i = \beta_i \ \ (\forall i,\ 1 \leq i \leq n, m)$.

Premièrement, on sait que :

$$p_i \text{ divise } p_1^{\alpha_1} \dots p_n^{\alpha_n} \ \ (\forall i,\ 1 \leq i \leq n)$$

mais par conséquent,

$$p_i \text{ divise aussi } q_1^{\beta_1} \dots q_m^{\beta_m} \ \ (\forall i,\ 1 \leq i \leq n)$$

(vu qu'ils sont censés être égaux)

Mais si on applique plusieurs fois le lemme d'Euclide, on déduit que :

$$\begin{aligned} & p_i \text{ divise } q_r^{\beta_r} \text{ (pour un certain } 1 \leq r \leq m) \\ \Longrightarrow\ & p_i \text{ divise } q_r \end{aligned}$$

(Note : Si ces deux assertions ne vous paraissent pas évidentes, il faut comprendre que le lemme d'Euclide s'étend à autant de facteurs que vous le voulez. Vu que p_i divise la décomposition de facteurs premiers, alors on sait que p_i divise **au moins un** des facteurs, d'où la précision de "un **certain** r". Et vu que p_i divise un nombre mis à une puissance, ce nombre n'a comme facteurs que lui même, d'où l'implication que p_i divise q_r)

Maintenant on sait que que p_i divise q_r, mais on rappelle que p et q sont des nombres **premiers**.

Par conséquent, ils ne possèdent aucun diviseur autre que 1 et eux-même, et vu que $p, q \neq 1$ (car 1 n'est pas considéré comme premier), on conclut que :

$$p_i = q_r$$

Mais si l'on répète ce processus pour chaque facteur des deux côtés de l'égalité, alors on observe qu'à chaque facteur p_i on peut associer un facteur q_r, et inversement.
Par conséquent, on conclut que :

$$n = m$$

et que les deux décompositions possèdent les mêmes nombres premiers en facteurs.

Maintenant que nous avons prouvé que les deux décompositions ont le même nombre de facteurs, et que ces facteurs sont égaux entre eux, il suffit de prouver que ces facteurs sont bien élevés aux mêmes puissances.
Après avoir réarrangé les termes, on a :

$$p_1^{\alpha_1} \dots p_n^{\alpha_n} = p_1^{\beta_1} \dots p_n^{\beta_n} \tag{1}$$

On cherche donc à montrer que :

$$\alpha_i = \beta_i \quad (\forall i,\ 1 \leq i \leq n)$$

Nous allons démontrer cela par l'absurde :
Assumons que $\alpha_i > \beta_i$
Divisons les deux côtés de l'égalité (1) par $p_i^{\beta_i}$. On obtient donc l'égalité suivante :

$$p_1^{\alpha_1} \dots p_i^{\alpha_i - \beta_i} \dots p_n^{\alpha_n} = p_1^{\beta_1} \dots p_{i-1}^{\beta_{i-1}} p_{i+1}^{\beta_{i+1}} p_n^{\beta_n} \tag{2}$$

(Note : si vous n'avez pas bien compris, vu que $\alpha_i > \beta_i$, alors du côté gauche le facteur p_i existe toujours, il a juste perdu en puissance, alors qu'à droite il a tout simplement disparu, emporté par la division.)

Avec l'égalité (2), on en déduit :

$$\begin{aligned} & p_i \text{ divise } p_1^{\alpha_1} \dots p_i^{\alpha_i - \beta_i} \dots p_n^{\alpha_n} \\ \implies & p_i \text{ divise } p_1^{\beta_1} \dots p_{i-1}^{\beta_{i-1}} p_{i+1}^{\beta_{i+1}} p_n^{\beta_n} \\ \implies & p_i \text{ divise } p_j \quad \text{avec } i \neq j \quad \text{(D'après le lemme d'Euclide)} \end{aligned}$$

Mais nous sommes face à une contradiction !
En effet, p_i **ne peut pas** diviser p_j, car ces deux nombres ont été définis comme premiers.
On en conclut donc que,

$$\alpha_i \not> \beta_i$$

et avec la logique inverse on pourrait aussi prouver que,

$$\alpha_i \not< \beta_i$$

Conclusion :

$$\alpha_i = \beta_i \ \ (\forall i,\ 1 \leq i \leq n)$$

Nous avons démontré que si deux décompositions sont égales, alors cela implique qu'elles aient le même nombre de facteurs, que ces facteurs soient égaux entre eux, et que ces mêmes facteurs soient élevés à une même puissance. De cela nous pouvons enfin conclure que :

La décomposition d'un nombre en facteurs premiers est unique.

□

2.2 Forme générale d'une décomposition

Maintenant que nous avons fini la démonstration, nous pouvons enfin énoncer le théorème :

Théorème 2.2.0.1. ***Théorème fondamental de l'arithmétique*** *:*
$\forall n \in \mathbb{N}\backslash\{0,1\}$, $\exists! k \in \mathbb{N}^*$ *avec* $p_1 \dots p_k$ *des nombres premiers et* $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$ *tel que :*

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

(Nous verrons des applications de ce théorème dans les sections 3.3.1 et 3.3.2)

3 Deux outils de l'arithmétique

3.1 Le PGCD : Plus Grand Commun Diviseur

Définition 3.1.0.1. Soient a et b deux entiers dont au moins l'un des deux est non nul. On appelle PGCD le Plus Grand Commun Diviseur de a et b. On note $a \bigwedge b$ le plus grand des diviseurs communs à a et b.

Propriétés 3.1.0.1. Montrons quelques propriétés du PGCD :

1. $\forall a \in \mathbb{N}^*$, PGCD(a,0) = a et PGCD(a,1) = 1
2. PGCD(a,b) = PGCD (b,a)
3. Si $(a, b, k) \in \mathbb{Z}^3$, $(ka) \bigwedge (kb) = |k|(a \bigwedge b)$, cela représente l'homogénéité du PGCD. Soit PGCD(ka,kb) = k × PGCD(a,b)
4. Si b $\in \mathbb{N}^*$, et si a = bq + r est la division euclidienne de a par b, alors $a \bigwedge b = b \bigwedge r$
5. Pour tout couple $(a, b) \in \mathbb{Z}^2$, il existe $(u, v) \in \mathbb{Z}^2$ tel que :
   $au + bv = a \bigwedge b$. Le couple (u,v) est appelé couple de coefficient de Bezout.
   Si $au + bv = 1$, on peut déduire que a et b sont premiers entre eux, c'est à dire que a ne divise pas b, et reciproquement que b ne divise pas a. (On appelle cette propriété : "Théorème de Bachet-Bézout"[22])

Exemple 3.1.0.1. Voici quelques exemples de PGCD :

PGCD(60,100) = 20

PGCD(252,360) = 36

PGCD(2730,5610) = 30

3.1.1 L'Algorithme d'Euclide

Définition 3.1.1.1. L'Algorithme d'Euclide est un algorithme permettant de calculer facilement le PGCD de deux nombres a et b. Pour cela, il faut calculer la division euclidienne de a par b. Ensuite a prend la valeur de b et b prend la valeur du reste. On répète l'opération jusqu'à ce que b soit égal à 0. On prend alors la valeur (finale) de a.
Pour mieux comprendre ce propos, en voici une illustration (Figure 3) ainsi qu'un exemple.

Exemple 3.1.1.1. PGCD(360, 252) :
$360 = 252 \times 1 + 108$
$252 = 108 \times 2 + 36$
$108 = 36 \times 3 + 0$
Le PGCD de 360 et 252 est 36.

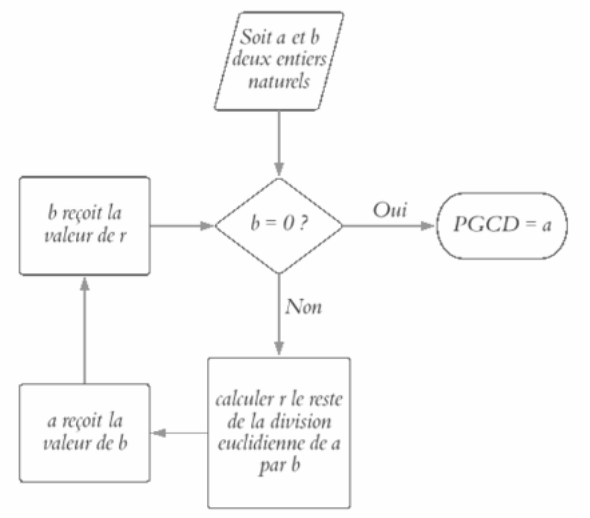

FIGURE 3 – Algorithme Euclide

3.2 Le PPCM : Plus Petit Commun Multiple

Le PPCM signifie Plus Petit Commun Multiple.

Définition 3.2.0.1. *Soient a et b deux entiers. Les assertions suivantes sont équivalentes :*

- *a est un multiple de b*
- *b est un diviseur de a*
- *b|a*
- $\exists k \in \mathbb{Z}$ *tel que* $bk = a$

Le PPCM de deux entiers a et b, noté $a \vee b$, est donc le plus petit entier naturel qui soit à la fois un multiple de a et de b.

Exemple 3.2.0.1. $3 \vee 5 = 15$ *;* $2 \vee 6 = 6$

Bien que moins étudié que le PGCD, le PPCM possède néanmoins lui aussi quelques propriétés intéressantes.

La plus notable est la suivante :

Théorème 3.2.0.1. *Soient $m = a \vee b$, et q un entier. On a alors :*
$(a|q)$ *et* $(b|q) \iff (m|q)$

3.3 Liens avec la décomposition en facteur premier

3.3.1 Calculer le PGCD à partir de la décomposition en facteurs premiers

Avoir la décomposition en facteurs premiers de deux nombres a et b permet de calculer très facilement leur PGCD $a \wedge b$.

Il suffit d'étudier chaque facteur commun aux décompositions de a et b, et de le prendre au plus petit exposant. En multipliant tous les facteurs retenus, nous obtenons le PGCD de a et b.

Prenons un exemple :

Exemple 3.3.1.1. *Posons $a = 792$ et $b = 2970$. On a :*
$a = 2^3 \times 3^2 \times 11$
$b = 2 \times 3^3 \times 5 \times 11$
Il devient très facile de calculer $a \wedge b = 2 \times 3^2 \times 11 = 198$.

Pour effectuer ce calcul, le raisonnement fut le suivant :

- 2 est un factuer commun aux décompositions de a et b. Dans la décomposition de a, il est à l'exposant 3, tandis qu'il est exposant 1 dans la décomposition de b. Nous prenons le plus petit exposant, on garde donc $2^1 = 2$.
- 3 est également un facteur commun aux deux décomositions. Il est au plus petit exposant dans celle de a, on retient donc 3^2.
- 5 n'est pas présent dans la décomposition de a, on ne le garde donc pas.
- 11 est un facteur commun aux deux décomposition. Il est en outre à l'exposant 1 dans les deux cas. On garde donc $11^1 = 11$.

D'où, en faisant le produit, $a \wedge b = 2 \times 3^2 \times 11$.

Démonstration. Le fonctionnement de cette méthode est assez intuitif, quand on comprend le sens de la décomposition en facteurs premiers. Une façon de le démontrer serait d'appeler m le nombre que nous trouvons avec cette technique, et d'ensuite étudier a et b divisés par m.

On remarquerait alors que a/m et b/m n'ont pas de diviseur commun autre que 1. D'après la propriété 3 :

$a \wedge b = (m\frac{a}{m}) \wedge (m\frac{b}{m}) = |m|(\frac{a}{m} \wedge \frac{b}{m}) = m \times 1 = m$ □

3.3.2 Calculer le PPCM à partir de la décomposition en facteurs premiers

La décomposition en facteurs premiers permet aussi, via une méthode à peu près similaire à celle vue ci-dessus, de calculer le PPCM de deux nombres.

La différence avec la méthode de calcul du PGCD est que, pour chaque facteur présent dans la décomposition en facteurs premiers de a **OU** b, on garde l'exposant le plus **grand**.

Reprenons l'exemple ci-dessus :

Exemple 3.3.2.1. *Prenons encore :*
$a = 792 = 2^3 \times 3^2 \times 11$ *et*
$b = 2970 = 2 \times 3^3 \times 5 \times 11$
On calcule alors : $a \vee b = 2^3 \times 3^3 \times 5 \times 11 = 11\ 880$.

3.4 Lien entre PGCD et PPCM

Une formule simple relie le PPCM et le PGCD de deux nombres :

Théorème 3.4.0.1.

$$PGCD(a,b) \times PPCM(a,b) = |ab|$$
$$\iff PGCD(a,b) = \frac{|ab|}{PPCM(a,b)}$$
$$\iff PPCM(a,b) = \frac{|ab|}{PGCD(a,b)}$$

Ce théorème, assez impressionant, peut en fait se comprendre assez facilement. C'est pourquoi nous allons l'illustrer avec un exemple.

Exemple 3.4.0.1. *Une fois n'est pas coutume, posons* $a = 792$ *et* $b = 2970$. *Regardons maintenant le tableau suivant, comparant l'exposition de chaque facteur dans les décompositions en facteurs premiers de* a, b, $a \wedge b$, $a \vee b$, $a \times b$ *et* $(a \wedge b) \times (a \vee b)$ *:*

Facteur	a	b	*pgcd*	*ppcm*	$a \times b$	*pgcd* $\times$ *ppcm*
2	*3*	*1*	*1*	*3*	*4*	*4*
3	*2*	*3*	*2*	*3*	*5*	*5*
5	*0*	*1*	*0*	*1*	*1*	*1*
11	*1*	*1*	*1*	*1*	*2*	*2*

En fait, on peut se représenter les choses en se disant que pour chaque facteur, le plus petit exposant entre a et b devient l'exposant du PGCD, et le plus grand devient celui du PPCM.

En rappelant que $n^a \times n^b = n^{(a+b)}$, on arrive très facilement à la proriété vue ci-dessus.

Toutefois, une démonstration complète peut être trouvée ici : [23]

4 Algorithme de Calcul de la décomposition en facteurs premiers

Dans cette partie, nous allons chercher à écrire un algorithme qui donne la décomposition en facteurs premiers d'un nombre. On en a déjà donné un avec l'algorithme d'Euclide, dans la partie 3.1.1. Toutefois, nous allons ici travailler avec plusieurs fonctions indépendantes et intermédiaires, pour élargir l'angle de compréhension des outils que nous avons vus dans les parties précédentes.

Pour qu'il soit aisément réutilisable, cet algorithme sera écrit comme un programme en langage python.

4.1 Identification d'un nombre premier

4.1.1 Principe de l'algorithme

Pour décomposer un nombre en facteurs premiers, il est nécessaire que notre programme puisse identifier un nombre comme étant premier. Grâce à la définition 1.0.0.1, nous pouvons déterminer deux caractéristiques des nombres premiers qui nous aideront dans la rédaction de notre programme :

1. Ils sont strictement supérieurs à 1.

2. Ils n'ont aucun diviseur strictement supérieur à 1.

Il est aussi important de noter que tester tous les entiers sur $]1, \sqrt{n}]$, est suffisant pour vérifier si n est premier.

Démontrons-le par l'absurde :

Démonstration. Soit r la racine carrée d'un entier n.
Soit a un diviseur de n. Par définition, $\exists\ b \in\ \mathbb{Z}$ tel que $ab\ =\ n$
Supposons $a > r$ et $b > r$
Alors $ab > r^2\ \iff\ ab > n$ □

La proposition est absurde. Par conséquent, à tout divseur a de n supérieur à la racine carrée de n est associé un diviseur b de n, inférieur ou égal à la racine carrée de n.

4.1.2 Programmation en python

En considérant ce qui a été vu plus haut, on peut écrire le programme suivant, qui détermine si un nombre n est premier :

```
def tester_nombre_premier(n) :
    if n <= 1 :
        est_premier = False
    else :
        est_premier = True
        for i in range (floor(sqrt(n)), 1, -1) :
            if n%i == 0 :
                est_premier = False
    return est_premier
```

4.2 Création d'une liste de nombres premiers potentiels diviseurs

Pour trouver la décomposition en facteurs premiers d'un nombre n, nous allons déterminer la liste exhaustive des nombres premiers qui peuvent potentiellement être des diviseurs de n.

Pour cela, nous allons récupérer tous les nombres premiers entre 1 et n.

Le programme en python est celui-ci :

```
def creer_liste_premiers(n) :
    liste_premiers = []
    for i in range (n, 1, -1) :
        if tester_nombre_premier(i) :
            liste_premiers.append(i)
    return liste_premiers
```

Note : *l'intérêt de passer par une telle fonction intermédiaire n'est pas évident. Le but de cette fonction, qui n'a pas été poussé ici, est de faciliter la récupération de listes complètes de nombres premiers, qui peuvent ensuite être aisément stockées sur des fichiers annexes. Ainsi, il serait facile d'optimiser grandement les calculs, en récupérant les listes déjà stockées. On n'aurait alors plus besoin de calculer de nouveaux nombres premiers que pour tester des nombres strictement supérieurs à tous ceux testés avant.*

4.3 Création d'une liste contenant la décomposition en facteurs premiers

Avec la liste des nombres premiers potentiellement diviseurs, il devient facile de récupérer la décomposition en facteurs premiers d'un nombre.

Il suffit d'essayer de diviser le nombre par chaque terme de la liste autant que possible, jusqu'à ce que le nombre vaille 1. Par définition, le nombre ne sera alors plus divisible.

Le programme python suivant permet donc de récupérer la décomposition en facteurs premiers d'un nombre n :

```
def decompo_premiers(n) :
    nombre_compose = n
    liste_premiers = creer_liste_premiers(n)
```

```
liste_decomposition = []
for i in liste_premiers :
    while nombre_compose%i == 0 :
        liste_decomposition.append(i)
        nombre_compose = nombre_compose/i
return liste_decomposition
```

4.4 Programme de calcul du PGCD

En utilisant ce que nous avons vu dans la partie 3.3.1, et le programme ci-dessus, il devient possible d'écrire un programme calculant le PGCD de deux nombres.

Pour le comprendre, il est important de se souvenir que le programme que nous avons écrit nous donne la décomposition en facteurs premiers d'un nombre sous la forme d'une liste. Ainsi, contrairement à la forme générale qui utilise une notation avec des exposants, la liste contiendra un facteur autant de fois qu'il interviendra dans la décomposition.

Exemple 4.4.0.1. *Le nombre 108, dans la forme générale de sa décomposition en facteurs premiers, s'écrit* $2^2 \times 3^3$. *La fonction que l'on a écrite, elle, nous renverra la liste* `[2, 2, 3, 3, 3]`

On peut donc tester un à un les facteurs de la décomposition d'un des deux nombres, et les multiplier au PGCD si et seulement si ce facteur se trouve également dans la décomposition de l'autre nombre.

Notons que :

- On supprime les facteurs de la liste du second nombre au fur et à mesure.
- Ainsi, le facteur est toujours compté le nombre minimum de fois :
  - S'il apparaît moins de fois dans la décomposition a, alors on arrêtera de le compter dès que la boucle aura parcouru toutes ses apparitions dans ladite décomposition.
  - S'il apparaît moins de fois dans la décomposition b, alors il sera enlevé autant de fois de la liste b, et la condition cessant alors d'être respectée, le facteur ne sera plus pris en compte aux prochains passages de la boucle.

- Pour simplifier les choses, le programme ici ne fonctionne qu'avec deux nombres strictement positifs. Autrement, la fonction retourne `None`.

```
def calcul_pgcd(a, b) :
    decompo_a = decompo_premiers(a)
    decompo_b = decompo_premiers(b)
    pgcd = None
    for i in decompo_a :
        if i in decompo_b :
            if pgcd is None :
                pgcd = 1
            pgcd *= i
            decompo_b.remove(i)
    return pgcd
```

4.5 Programme de calcul du PPCM

4.5.1 Programme indépendant

À partir de ce que nous avons vu dans la partie 3.3.2, il est possible d'écrire un programme calculant le ppcm de deux nombres, avec un fonctionnement assez similaire au programme de calcul du PGCD que nous avons vu.

Seulement, pour le calcul du ppcm, on cherche à compter chaque facteur le nombre **maximal** de fois où il intervient.

On décompose donc le programme en deux étapes :

1. On compte chaque facteur de la première décomposition autant de fois qu'il apparaît, en le supprimant (quand il y est) de la liste de la seconde décomposition.

2. S'il reste des facteurs dans la liste de la seconde décomposition, on les multiplie au PPCM.

Ainsi, on est sûr d'avoir bien pris en compte chaque terme le plus grand nombre de fois.

Voici donc le programme qui, comme celui du PGCD que nous avons vu, ne fonctionne que pour a et b strictement positifs.

```
def calcul_ppcm(a, b) :
    decompo_a = decompo_premiers(a)
    decompo_b = decompo_premiers(b)
    ppcm = None
    for i in decompo_a :
        if ppcm is None :
            ppcm = 1
        ppcm *= i
        if i in decompo_b :
            decompo_b.remove(i)
    for j in decompo_b :
        if not (ppcm is None) :
            ppcm *= j
    return ppcm
```

4.5.2 Programme utilisant celui calculant le PGCD

Comme nous l'avons vu avec le théorème 3.4.0.1, il est possible de calculer le PPCM à partir du PGCD. En utilisant le programme qui calcule le PGCD, il suffit en fait d'exploiter cette formule, pour créer un programme calculant facilement le PPCM de deux nombres a et b strictement positifs :

```
def calcul_simple_ppcm(a, b) :
    return (a*b)/calcul_pgcd(a, b)
```

références

Note : les références sont cliquable.

[1] Wikipédia, entier naturel.

[2] Wikipédia, Groupes.

[3] Techno-Science.net, Bijection - Définition et Explications.

[4] Wikipédia, Argument de la diagonale de Cantor.

[5] Wikipédia, Hypothèse du continu.

[6] Wikipédia, Euclide.

[7] UJF Grenoble, démonstration de la division euclidienne.

[8] Wikipédia, arithmétique modulaire.

[9] Wikipédia, théorie algébrique des nombres.

[10] Wikipédia, arithmétique des polynômes.

[11] Wikipédia, Crise des fondements.

[12] Wikipédia, Giuseppe Peano.

[13] Wikipédia, Axiome.

[14] Wikipédia, système axiomatique.

[15] Wikipédia, Théorie des ensembles de Zermelo-Fraenkel.

[16] Wikipédia, Calcul des prédicats.

[17] Futura sciences, Théorèmes d'incomplétude de Gödel.

[18] Alain Kraus, cours arithmétique page 9, théoreme 1.2

[19] M@ths et tiques, histoire des nombres premiers.

[20] Michael Penn, Number Theory | Fundamental Theorem of Arithmetic

[21] PDF, Le lemme d'Euclide

[22] Wikipédia, Théorème de Bachet-Bézout.

[23] Wikipédia, Calcul du PPCM à l'aide du PGCD

[24] Livre, "Tout ce qu'il faut savoir sur les mathématiques", Jacques Delfaud, MPSI-MP2I