Introduction à l'arithmétique
L1ME

Ismaïla DIOUF

31 août 2012

Table des matières

Chapitre 1

L'ensemble $\mathbb{N}$ et l'ensemble $\mathbb{Z}$

Introduction

L'arithmétique est la science des nombres, plus précisément des nombres entiers, qu'ils soient naturels : $0, 1, 2, ...$ ou relatifs $-1, 0, 1, 2, ...$ Les outils essentiels sont les quatre opérations : addition, soustraction, multiplication et division auxquelles il faut ajouter la relation d'ordre $\leqslant$. L'objectif poursuivi dans ce cours n'est pas d'étudier $\mathbb{N}$ et $\mathbb{Z}$ «pour eux-mêmes», mais en liaison avec les nombreux domaines des mathématiques (ou de leurs applications) où ils interviennent. Citons quelques raisons de s'intéresser aux entiers.

1. Ils servent d'abord à compter (c'est leur fonction cardinale), ou à numéroter des objets (c'est leur fonction ordinale). On est familiarisé avec ces deux fonctions depuis notre enfance. Et depuis peu, avec l'aspect d'ensemble infini : après n'importe quel entier, il en existe toujours au moins un plus grand.
2. Dans toutes les branches des mathématiques, l'un des modes de raisonnement fondamentaux est le raisonnement par récurrence, dans lequel l'intervention de $\mathbb{N}$ est évidente. À cet égard, l'arithmétique elle-même a le mérite d'offrir de nombreux exemples de tels raisonnements, qu'ils soient très simples ou plus élaborés.
3. Les ordinateurs manient des nombres entiers (écrits en système binaire). Ils ne font même que cela mais pas n'importe comment : ils sont programmés. Lorsqu'ils effectuent un programme, ils passent d'une instruction n à l'instruction suivante $n+1$, démarche proche de celle que l'on suit dans un raisonnement par récurrence. Dans les programmes on fait appel à des algorithmes, i.e des procédés de calcul, et ces algorithmes portent souvent sur des entiers. Il peut être important de comprendre ou de savoir se servir de ces algorithmes et, si nécessaire, de mettre au point un algorithme répondant à tel ou tel besoin. À l'inverse, savoir écrire un programme (fonctionnant correctement) qui résout un certain problème mathématique prouve au moins que l'on a compris les notions intervenant dans ce problème.
4. En ce qui concerne $\mathbb{Z}$, son étude a ici une motivation directe. D'abord chacun pourra constater que l'algèbre (notamment l'algèbre linéaire) occupe une place importante dans l'enseignement des mathématiques. Il s'agit d'un outil puissant, utilisé dans beaucoup de domaines des mathématiques et de leurs applications. L'algèbre met en jeux des objets fondamentaux, tels que les groupes ou les anneaux. Dans chacun de ces cas, $\mathbb{Z}$ offre l'exemple le plus simple du type d'objet envisagé.

1.1 Entiers naturels

L'ensemble, noté $\mathbb{N}$, des entiers naturels peut être défini par cinq axiomes dégagés par Peano.

1. Zéro, noté 0, est un entier.
2. Tout entier n a un successeur («suivant») qui est un entier noté n^+ (en particulier le successeur de 0 est noté $0^+ = 1$). n est le prédecesseur de n^+.
3. Zéro n'est pas un successeur.
4. Deux entiers sont égaux ssi leurs successeurs le sont.
5. Soit $\mathscr{P}(n)$ une propriété relative à l'entier n. Supposons que la propriété soit vraie pour l'entier 0 et que l'on puisse établir que la propriété supposée vraie pour l'entier n l'est aussi pour l'entier n^+ : $\mathscr{P}(n)$ est vraie pour tout n.

Ce cinquième axiome est connu sous le nom de «principe d'induction complète» et il est à la base du raisonnement par récurrence. Nous supposons connues les propriétés élémentaires de l'ensemble $\mathbb{N}$ ainsi que les opérations usuelles.

Dans la section suivante, nous donnons une construction de $\mathbb{Z}$, à partir de $\mathbb{N}$.

1.2 L'anneau $\mathbb{Z}$ des entiers relatifs

La différence de deux entiers naturels a et b : $d = a - b$ ne peut être définie que si $a \geqslant b$ (dans $\mathbb{N}$). On se propose, en étendant convenablement l'ensemble $\mathbb{N}$, de supprimer cette restriction.

Si c est un entier naturel tel que : $c \leqslant b \leqslant a$, il clair que :

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

Exemple 1.

$$5 = 7 - 2 = 8 - 3 = 9 - 4.$$

Plus généralement, tout entier naturel n peut d'une infinité de manières s'écrire sous forme d'une différence :

$$n = a - b = a' - b' = a'' - b'' \ldots (a \geqslant b, \quad a' \geqslant b' \ldots).$$

On peut convenir d'identifier les couples $(a,b), (a',b'), \ldots$ de même différence et d'écrire :

$$n = (a,b) = (a',b') = \ldots \tag{1.1}$$

De $a - b = a' - b'$, on déduit en ajoutant $b + b'$ aux deux membres :

$$a + b' = a' + b. \tag{1.2}$$

Ainsi, (2.2) implique (1.2) mais la réciproque n'est pas vraie : (1.2) n'implique nullement $a \geqslant b, a' \geqslant b'$, conditions d'ailleurs nécessaires et suffisantes pour qu'on puisse déduire (1.2) de (2.2).

Exemple 2.

$$1 + 6 = 2 + 5 \quad \text{n'équivaut pas} \quad 1 - 5 = 2 - 6$$

expression qui n'a aucun sens dans $\mathbb{N}$.

1.2.1 L'ensemble $\mathbb{Z}$

La relation (1.2), plus générale que (2.2), permet de définir entre les couples d'entiers naturels ordonnés une relation d'équivalence, notée provisoirement $\mathfrak{R}$.
En effet, l'écriture $(a,b)\,\mathfrak{R}\,(a',b')$ si $a+b'=a'+b$ détermine entre de tels couples une relation $\mathfrak{R}$, qui est :

a **reflexive** $\quad (a,b)\,\mathfrak{R}\,(a,b) \quad (a+b=b+a)$

b **symétrique** $\quad (a,b)\,\mathfrak{R}\,(a',b') \quad (a'+b=b'+a)$

c **transitive** en effet, $\quad (a,b)\,\mathfrak{R}\,(a',b')$, et $(a',b')\,\mathfrak{R}\,(a'',b'')$

On a $a+b'=a'+b$ et $a'+b''=a''+b'$, on déduit en ajoutant membre à membre :

$$a+b'+a'+b''=a'+b+a''+b'$$

ou

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

En retranchant $a'+b'$ aux deux membres on obtient $(a,b)\,\mathfrak{R}\,(a'',b'')$.

Une classe d'équivalence de $\mathfrak{R}$ est l'ensemble de tous les couples ordonnés qui sont dans la relation $\mathfrak{R}$ avec l'un quelconque d'entre eux, choisi comme «représentant».
Ainsi, $(3,1),(2,0),(7,5)$ appartiennent à une même classe de représentant $(2,0)$.
Tout couple d'entiers naturels ordonnés appartient à une classe et une seule.
L'ensemble de toutes ces classes est désigné par $\mathbb{Z}$.

1.2.2 Propriété de $\mathbb{Z}$

Soit $(a,b)\in\mathbb{Z}$. Si $a>b$, posons $d=a-b$; on a : $d+b=a+0$, donc $(d,0)\,\mathfrak{R}\,(a,b)$. Or l'application $(d,0)\mapsto d$ est une bijection de l'ensemble des couples ordonnés, dont le premier élément est un nombre naturel et le dernier 0, sur l'ensemble $\mathbb{N}$ des nombres naturels, en sorte qu'ont peut convenir d'écrire plus simplement :

$$d\,\mathfrak{R}\,(a,b).$$

Ainsi, pour les couples ordonnés (a,b) tels que $a>b$, la relation $\mathfrak{R}$ n'est autre que la relation d'égalité et les entiers naturels, des représentants des diverses classes de tels couples : on les nomme entiers positifs.

Donc on a $\mathbb{N}\subset\mathbb{Z}$ et il est légitime de remplacer la notation $\mathfrak{R}$ par la notation "=".

$a=b \quad (a,b)=(a-b,a-b)=(0,0)=0.$

$a<b \quad (a,b)=(a-a,b-a)=(0,b-a).$

Un tel couple dont le premier élément est nul est le représentant d'une classe dite «entier négatif».

Désormais l'ensemble $\mathbb{N}$ et celui des entiers négatifs seront dits constituer l'ensemble $\mathbb{Z}$ des entiers relatifs, ou nombres entiers relatifs.

1.2.3 Addition et soustraction de deux entiers relatifs

Entre deux éléments quelconques de $\mathbb{Z}$, (a,b) et (c,d), définissons une loi de composition (notée $+$) associant à ces éléments un troisième dit «somme» par l'égalité :

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

a). Cette loi est compatible avec la notion de classes de couples, i.e que l'égalité précédente subsiste quand on remplace (a,b) par $(a',b') = (a,b)$.

b). La loi est commutative.

c). Il existe pour cette loi un élément neutre unique $(0,0) = 0$.

d). L'opération inverse de l'addition ou soustraction est toujours possible.
Étant donné deux couples (a,b) et (c,d), montrons qu'il existe (x,y) définissant un nombre relatif unique tel que :

$$(c,d) + (x,y) = (a,b)$$

ou bien

$$(c+x, d+y) = (a,b) \tag{1.3}$$

Notation : $(x,y) = (a,b) - (c,d)$: (x,y) est la différence entre (a,b) et (c,d). En effet, (1.3) équivaut à $b+c+x = a+d+y$. Donc :
– Si $a+d < b+c$, on choisit $x = 0$ et $y = (b+c) - (a+d)$;
– Si $a+d > b+c$, on choisit $y = 0$ et $x = (a+d) - (b+c)$;
– Si $a+d = b+c$, on choisit $x = 0$ et $y = 0$.
En particulier, il existe (x,y) unique tel que :

$$(a+b) + (x+y) = 0.$$

– Si $a \geqslant b$, alors $(a,b) = (a-b,0)$ et $(x,y) = (0,a-b)$.
– Si $a < b$, alors $(a,b) = (0,b-a)$ et $(x,y) = (b-a,0)$.
L'entier relatif (x,y) ainsi défini est dit opposé de (a,b).

Remarque. (a,b) et (b,a) sont opposés.

e). La loi est évidemment associative.

En somme, cette loi est une loi de groupe commutatif (ou abélien).

1.2.4 Écriture conventionnelle des entiers relatifs

Tout entier relatif non nul admet un représentant du type $(n,0)$ ou $(0,n)$ avec : $n \neq 0 \in \mathbb{N}$.
On convient d'écrire :
$(n,0) = (+n)$ entier positif noté aussi n par abus d'écriture.
$(0,n) = (-n)$ entier négatif.
n est la valeur absolue de $(+n)$ ou de $(-n)$, notée :

$$n = |(+n)| = |(-n)|.$$

Grâce à cette convention, on peut établir facilement les règles suivantes :

RÈGLE 1. La somme de deux entiers relatifs de même signe est un entier relatif ayant pour valeur absolue la somme des valeurs absolues et pour signe le signe commun.

Exemple 3.

$$(+5) + (+2) = (+7) \qquad (-4) + (-6) = (-10).$$

RÈGLE 2. La somme de deux entiers relatifs de signes contraires est un entier relatif ayant pour valeur absolue la différence des valeurs absolues et pour signe celui de l'entier ayant la plus grande valeur absolue.

Exemple 4.

$$(+5)+(-2)=(+3) \qquad (+4)+(-6)=(-2).$$

RÈGLE 3. Pour retrancher un entier relatif d'un autre entier relatif relatif, on ajoute à ce dernier l'opposé du premier.

Exemple 5.

$$(+5)-(+8)=(+5)+(-8)=-3, \qquad (+4)-(-3)=(+4)+(+3)=(+7).$$

1.2.5 Simplification d'écriture

On peut simplifier l'écriture des opérations précédentes, en combinant les signes opératoires avec les signes intérieurs aux parenthèses.

$$\begin{array}{lll} + \text{ par } + & \text{donne} & + \\ - \text{ par } - & \text{donne} & + \\ + \text{ par } - & \text{donne} & - \\ - \text{ par } + & \text{donne} & - \end{array}$$

Exemple 6.

$$5-8=-3, \qquad 4+3=7.$$

1.2.6 Propriétés de la multiplication

Soient (a,b) et (c,d) les représentants de deux entiers relatifs donnés. On leur associe un nombre relatif dit produit :

$$(ac+bd,bc+ad),$$

la loi de composition correspondante étant dite «multiplication» et on écrit :

$$(a,b)\times(c,d)=(a,b)\cdot(c,d)=(ac+bd,bc+ad).$$

Observons que cette loi de composition contient comme cas particulier le produit de deux entiers naturels. En effet, si a et $c\in\mathbb{N}$, on a :

$$(a,0)\cdot(c,0)=(ac,0)$$

On montre que cette loi est compatible avec la relation d'équivalence définie sur $\mathbb{Z}$, i.e qu'on obtient encore le même entier relatif, quand on remplace (a,b) par $(a',b')=(a,b)$. Pour ce qui est du produit de deux entiers relatifs on aboutit à la règle suivante :

RÈGLE 4. Le produit de deux entiers relatifs est un entier relatif dont la valeur absolue est le produit des valeurs absolues et dont le signe est $+$, s'ils ont même signe, et $-$, s'ils sont de signes contraires. Il est donc commutatif.

a). La multiplication est partout définie et associative.

b). $(1,0)$ est l'élément neutre pour cette loi.

c). La multiplication est distributive par rapport à l'addition.

d). Par contre, (a,b) étant donné, il n'est pas possible en général de trouver $(x,y) \in \mathbb{Z}$ tel que : $(a,b) \cdot (x,y) = (1,0)$.

En résumé, sur $\mathbb{Z}$ on a défini deux lois de composition :

1) Une loi de groupe abélien notée $+$, ou addition.

2) Une multiplication notée $\times$ ou $\cdot$ qui est commutative, associative, distributive par rapport à l'addition.

On dit que ces deux lois définissent sur $\mathbb{Z}$ une structure d'anneau commutatif unitaire (il y a un élément neutre pour la multiplication). Nous ne reviendrons pas sur la notion d'ordre dans $\mathbb{Z}$, sur les propriétés des inégalités entre entiers relatifs ou autres de ce genre. Ces notions étant supposées connues et maîtrisées.

Chapitre 2

Arithmétique dans $\mathbb{Z}$

2.1 Divisibilité dans $\mathbb{Z}$

Rappelons que $(\mathbb{Z},+,\times)$ est un anneau commutatif. L'ensemble $a\mathbb{Z}$ est défini par : $a\mathbb{Z} = \{ak : \ k \in \mathbb{Z}\}$ et pour tous entiers relatifs a et b, on pose

$$a\mathbb{Z} + b\mathbb{Z} = \{ak + bl : \ k \in \mathbb{Z}, \ l \in \mathbb{Z}\}.$$

Nous ne reprendrons pas la preuve du théorème suivant (revoir le cours d'algèbre fondamental sur les anneaux).

Théorème 2.1. *Les idéaux de l'anneau $(\mathbb{Z},+,\times)$ sont exactement les sous-ensemble de $\mathbb{Z}$ de la forme $m\mathbb{Z}$, où $m \in \mathbb{Z}$.*

Plus précisément, pour tout idéal I de l'anneau $(\mathbb{Z},+,\times)$, il existe un unique $m \in \mathbb{N}$ tel que $I = m\mathbb{Z}$. Bien que déjà définie dans le cours d'algèbre fondamental sur un anneau intègre quelconque, nous allons rappeler la relation de divisibilité sur $(\mathbb{Z},+,\times)$ ainsi que ses principales propriétés.

2.1.1 Relation de divisibilité sur $\mathbb{Z}$

.

Définition 1. Soit $(a,b) \in \mathbb{Z}^2$, on dit que a **divise** b et on note $a|b$ s'il existe $q \in \mathbb{Z}$ tel que $b = aq$. On dit aussi que b est un multiple de a et on note quelquefois $b \vdots a$ (notation pas très fréquente).
Soit $n \in \mathbb{N}$, on dit que a^n **divise exactement** b ssi $a^n|b$ et $a^{n+1} \not| b$.
a^n divise exactement b se note par $a^n \parallel b$.

Remarques.

- Ainsi, 0 est divisible par n'importe quel entier relatif mais 0 ne divise aucun entier relatif non nul (0 ne divise que lui-même).
- Les seuls diviseurs dans $\mathbb{Z}$ de 1 sont 1 et -1.
- Pour tous entiers relatifs a et b, si $a|b$ alors $b\mathbb{Z} \subset a\mathbb{Z}$.

– La relation de divisibilité est réflexive et transitive mais pas antisymétrique sur $\mathbb{Z}$: on exprime cela en disant que c'est un **préordre**. En effet, $a|b$ et $b|a \iff a = \pm b$ (en effet, $a = bq = aq'q \Rightarrow qq' = 1 \Rightarrow q = q' = \pm 1$).

Notations. D'une manière générale, nous noterons $\mathscr{D}_{a_1,\ldots,a_m}$, l'ensemble des diviseurs communs aux entiers relatifs a_1, a_2, ..., a_m donnés. Ainsi, $\mathscr{D}_a$ désigne l'ensemble des diviseurs de a et on a

$$\mathscr{D}_{a_1,\ldots,a_m} = \mathscr{D}_{a_1} \cap \mathscr{D}_{a_2} \cap \cdots \cap \mathscr{D}_{a_m}.$$

De même $\mathscr{M}_{a_1,\ldots,a_m}$ sera l'ensemble des multiples communs aux entiers relatifs a_1, a_2, ..., a_m donnés. Ainsi, $\mathscr{M}_a$ désigne l'ensemble des multiples de a et on a

$$\mathscr{M}_{a_1,\ldots,a_m} = \mathscr{M}_{a_1} \cap \mathscr{M}_{a_2} \cap \cdots \cap \mathscr{M}_{a_m}.$$

L'ensemble $\mathscr{M}_a$ sera de préférence noté $a\mathbb{Z}$. Et donc,

$$\mathscr{M}_{a_1,\ldots,a_m} = a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}.$$

Deux entiers ont les mêmes diviseurs ssi ils sont associés [1] (dans $\mathbb{Z}$, i.e égaux ou opposés) :

Lemme 2.2. *On a $\mathscr{D}_a = \mathscr{D}_b$ si, et seulement si $a = \pm b$.*

Démonstration. Si $\mathscr{D}_a = \mathscr{D}_b$, alors $a \in \mathscr{D}_a = \mathscr{D}_b$ donc $a|b$. On prouve de même que $b|a$ d'où $a = \pm b$. La réciproque est évidente. □

Exemple 7. Soit $n \in \mathbb{N}^*$. Montrer que $9|10^n - 1$.

Solution. On a : $10^n - 1 = 9(10^{n-1} + 10^{n-2} + \cdots + 10 + 1)$ et donc le résultat s'ensuit. □

Exemple 8. On a $2^7|5^{2^5} - 1$. En effet, $5^{2^5} - 1 = (5-1)\prod_{k=0}^{4}(5^{2^k}+1) = 2^2\prod_{k=0}^{4}(5^{2^k}+1)$, chaque facteur dans le produit est pair. Donc ce produit est divisible par 2^5 au moins. D'où le résultat.

2.1.2 Le théorème de la division euclidienne

Le théorème de la division euclidienne est une mise en forme de la division enseignée et pratiquée dans les petites classes.

Nous prendrons pour acquis le principe du bon ordre qui s'énonce ainsi.

(Principe du bon ordre). Tout ensemble non vide $S \subset \mathbb{N}$ contient un plus petit élément.

Théorème 2.3 (Division euclidienne). *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leqslant r < b$. L'entier q est appelé le* **quotient** *de la division euclidienne de a par b et r est le* **reste** *de la division euclidienne de a par b.*

1. Soient A un anneau et $a, b \in A$, a et b sont dits associés ssi $aA = bA$.

Démonstration. **Unicité :** Soient (q_1, r_1) et (q_2, r_2) deux couples satisfaisant la relation $a = bq_1 + r_1 = bq_2 + r_2$. On a $b(q_1 - q_2) = r_2 - r_1$, ce qui veut dire que $b|(r_2 - r_1)$. Or $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$, il vient $-b < r_2 - r_1 < b$. Le seul multiple de b dans $]-b, b[$ est 0. Donc $r_1 = r_2 = 0$ et ainsi $q_1 = q_2 = 0$.
Existence : soit $E = \{a - kb : \ a - kb \geqslant 0, \ k \in \mathbb{Z}\}$. $E \neq \emptyset$ et $E \subset \mathbb{N}$ donc possède un plus petit élément, soit $r \geqslant 0$ cet élément. Notons q l'élément k associé à r. On a $a - bq = r$ i.e $a = bq + r$; montrons que $r < b$. Si $r \geqslant b$, alors $a - bq \geqslant b$ d'où $a - (q+1)b \in E$ et $a - (q+1)b < a - qb$ contradiction car $a - qb$ est le plus petit élément de E. □

Remarque.
- Le reste r est toujours un entier positif.
- Dans le théorème, il est clair que si $r = 0$, alors $b|a$ et inversement.
- Il est clair que si $a \in \mathbb{N}$, le quotient q dans la division euclidienne de a par b est aussi un entier naturel $(q \in \mathbb{N})$.
- Dans l'énoncé de la division euclidienne, on avait supposé $b > 0$. Qu'obtient-on lorsque $b < 0$? Dans cette situation, $-b$ est positif, et alors on peut appliquer la division euclidienne à a et $-b$. Par conséquent, il existe des entiers q et r tels que

  $$a = q(-b) + r, \qquad 0 \leqslant r < |b| .$$

  Or, cette relation peut s'écrire $a = (-q)b + r$, où, bien sûr, $-q$ est un entier. La conclusion est que la division euclidienne peut s'énoncer sous la forme plus générale : soient $a, b \in \mathbb{Z}$ avec $b \neq 0$, alors il existe des entiers q et r tels que $a = bq + r$, $0 \leqslant r < |b|$. De plus, si $b \nmid a$, alors $0 < r < |b|$.

Exemple 9.
- $a = 18, \ b = 7$, On a $18 = 2 \times 7 + 4$, i.e $q = 2$ et $r = 4$ $(0 \leqslant 4 < 7)$.
- $a = -12, \ b = 7$, on a $-12 = -2 \times 7 + 2$, i.e $q = -2$ et $r = 2$ $(0 \leqslant 2 < 7)$.

Exemple 10. Soit $n \in \mathbb{N}$. Écrire la division euclidienne de $n^3 + n^2 + 2n + 1$ par $n + 1$.

Solution. On a $n^3 + n^2 + 2n + 1 = (n+1)(n^2+1) + n$. □

2.1.3 Application aux systèmes de numération

Une importante application de la division euclidienne est la représentation d'entiers dans une base positive. Par exemple, tout entier positif n peut être représenté uniquement dans la base 10 comme suit

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0, \quad 0 \leqslant a_i \leqslant 9, \quad 0 \leqslant i \leqslant k.$$

En effet, étant donné un entier n, il existe un unique entier a_0 tel que $n = 10q + a_0$, $0 \leqslant a_0 \leqslant 9$. Par la suite nous divisons l'entier q par 10 pour obtenir $q = 10q_1 + a_1$ avec $0 \leqslant a_1 \leqslant 9$ et ainsi $n = 10^2 q_1 + 10a_1 + a_0$. En continuant le procédé, nous obtenons la représentation de n dans la base 10. La même technique nous amène facilement à montrer qu'un entier n a une représentation unique dans la base b :

Proposition 2.4. *Soient $n \in \mathbb{N}$ et $b \geqslant 2$. Il existe un unique entier naturel m et un unique $m+1$-uplet $(a_0, a_1, \ldots, a_m)$ d'entiers appartenant à $\{0, 1, \ldots, b-1\}$ tels que*

$$n = a_0 + a_1 b + a_2 b^2 + \cdots + a_m b^m, \quad m \neq 0,$$

*ce que l'on écrit de manière condensée $n = \underline{a_m \ldots a_1 a_0}_b$. On dit qu'il s'agit du **développement en base** b de l'entier naturel n.*

Démonstration. Notons r_0 le reste et q_0 le quotient dans la division euclidienne de n par b, puis, $\forall\, n \geqslant 1$, notons r_n le reste et q_n le quotient dans la division euclidienne de q_{n-1} par b. Il est clair que $(r_n)_n$ et $(q_n)_n$ sont deux suites à valeurs dans $\mathbb{N}$.

- **Unicité :** Les a_i sont uniques car, en cas d'existence, on a clairement $\forall\, k \leqslant m, a_k = r_k$ et $\forall\, k \geqslant m+1,\ r_k = 0$. L'entier m est donc le plus grand entier naturel k tel que $r_k \neq 0$.
- Montrons par l'absurde qu'il existe un entier n_0 pour lequel $q_{n_0} = 0$. Si ce n'était pas le cas on aurait, pour tout $n \geqslant 0$, $q_n = bq_{n+1} + r_{n+1}$ avec $r_{n+1} \geqslant 0$ et $bq_{n+1} \leqslant q_n$ et comme $q_{n+1} > 0$ et $b_n \geqslant 1$, $q_{n+1} < q_n$. La suite $(q_n)_n$ serait donc strictement décroissante ce qui est absurde car il s'agit d'une suite d'entiers naturels.
- **Existence :** Soit n_0 le plus petit entier naturel tel que $q_{n_0} = 0$. On a alors, pour tout $0 \leqslant k \leqslant q_{n_0}$, $q_k = bq_{k+1} + r_k$ et $q_{n_0} = 0$ d'où $n = r_0 + r_1 b + r_2 b^2 + \cdots + r_{n_0} b^{n_0}$. Le nombre r_{n_0} n'est pas nul car $q_{n_0-1} = bq_{n_0} + r_{n_0} = r_{n_0}$ et $q_{n_0-1} \neq 0$ par définition de n_0. □

Exemple 11. Écrivons $n = 10043$ en base 2.

Solution. On a successivement

$$\begin{aligned}
10043 &= 2 \times 5021 + 1,\\
5021 &= 2 \times 2510 + 1,\\
2510 &= 2 \times 1255 + 0,\\
1255 &= 2 \times 627 + 1,\\
627 &= 2 \times 313 + 1,\\
313 &= 2 \times 156 + 1,\\
156 &= 2 \times 78 + 0,\\
78 &= 2 \times 39 + 0,\\
39 &= 2 \times 19 + 1,\\
19 &= 2 \times 9 + 1,\\
9 &= 2 \times 4 + 1,\\
4 &= 2 \times 2 + 0,\\
2 &= 2 \times 1 + 0,\\
1 &= 2 \times 0 + 1.
\end{aligned}$$

Ainsi,

$$n = \underline{10043}_{10} = \underline{10011100111011}_2$$

Principe : On applique la méthode des divisions successives jusqu'à obtenir un quotient $q_{n_0} = 0$. On obtient alors en écrivant les restes par «remontée» :

$$n = \underline{r_{n_0} r_{n_0-1} \ldots r_1 r_0}_b$$

Exos 1. (a) Écrire $n = \underline{10111}_{10}$ en base 3. (on trouve : $\underline{111212111}_3$)

(b) Écrire $n = \underline{110011}_2$ en base 6. (on trouve : $\underline{123}_6$)

(c) Écrire $3n$ en base 3 où $n = \underline{21001}_3$ sans aucun calcul. (on trouve : $\underline{210010}_3$)

(d) Écrire $n+m$ en base 4 où $n = \underline{31231}_4$ et $m = \underline{20123}_4$. (on trouve : $\underline{112020}_4$)

2.1.4 Congruences dans $\mathbb{Z}$

L'idée de base des congruences est de faire de l'arithmétique avec les restes obtenus par la division de différents entiers.

Soit n un entier relatif non nul. La relation binaire $\mathfrak{R}$ définie sur $\mathbb{Z}$ par :

$$a \mathfrak{R} b \Longleftrightarrow n \,|\, a-b,$$

est d'équivalence (à prouver !).

Définition 2. Deux entiers relatifs a et b sont dits *congrus modulo n* ssi n divise $a-b$. Si tel est le cas, on écrit

$$a \equiv b \pmod{n}, \tag{2.1}$$

et on lit, «a et b sont congrus modulo n». Une relation du type (2.1) s'appelle une *congruence modulo n* ; l'entier n s'appelle le *module* de la congruence.

Il est clair que la relation de congruence modulo n est la même chose que la congruence modulo $(-n)$, et que $a \equiv b \pmod{n}$ équivaut à $a-b \in n\mathbb{Z}$. En particulier, si $n=0$, la congruence modulo 0 n'est autre que l'égalité dans $\mathbb{Z}$.

Un entier relatif m est divisible par n ssi $m \equiv 0 \pmod{n}$. Si q et r désignent respectivement le quotient et le reste de la division euclidienne de a par b $(\neq 0)$, alors on a $a \equiv r \pmod{b}$ mais également $a \equiv r \pmod{q}$. On retiendra le lemme suivant :

Lemme 2.5. *Si $a \equiv r \pmod{b}$, avec $b \in \mathbb{N}^*$ et $0 \leqslant r < b$, alors r est le reste de la division euclidienne de a par b.*

Voici quelques propriétés élémentaires des congruences très utiles pour nous aider dans les calculs :

Proposition 2.6. *Pour a, a', b, $b' \in \mathbb{Z}$:*

i) *Compatibilité de la congruence avec l'addition :*

$$\left.\begin{array}{ll} a \equiv a' & \pmod{n} \\ b \equiv b' & \pmod{n} \end{array}\right\} \Longrightarrow a+b \equiv a'+b' \pmod{n}$$

ii) *Compatibilité de la congruence avec la multiplication :*

$$\left.\begin{array}{ll} a \equiv a' & \pmod{n} \\ b \equiv b' & \pmod{n} \end{array}\right\} \Longrightarrow ab \equiv a'b' \pmod{n}$$

iii) *Pour tout $k \in \mathbb{N}$,*

$$a \equiv b \pmod{n} \Longrightarrow a^k \equiv b^k \pmod{n}.$$

iv) *Pour tout $\lambda \in \mathbb{N}^*$,*

$$a \equiv b \pmod{n} \Longrightarrow \lambda a \equiv \lambda b \pmod{\lambda n}.$$

v) *Si n' divise n alors :*

$$a \equiv b \pmod{n} \Longrightarrow a \equiv b \pmod{n'}.$$

vi) *Soit $d \neq 0$. Si d divise a, b et n, alors :*

$$a \equiv b \pmod{n} \Longrightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{n/d}.$$

Mais attention ! si $d \neq 0$ divise seulement a et b, la congruence $a \equiv b \pmod{n}$ n'entraîne pas en général $\frac{a}{d} \equiv \frac{b}{d} \pmod{n}$. Par exemple, prendre $a = 60$, $b = 40$, $n = 2$ et $d = 4$.

Démonstration. Facile, il suffit pratiquement d'utiliser la définition de la congruence. À faire en exo ! □

On pourrait être porté à croire que les congruences se comportent toujours comme des égalités. Or, il n'en est rien. Ainsi, lorsque $a \neq 0$, on a bien que $ax = ay \Longrightarrow x = y$; mais qu'advient-il si $ax \equiv ay \pmod{m}$? Par exemple, la congruence $21 \equiv 7 \pmod{14}$ devient, en enlevant le facteur 7, $3 \equiv 1 \pmod{14}$, ce qui est faux. De la même manière, $2 \equiv 12 \pmod{10}$ et $2 \equiv 12 \pmod{5}$ mais $2 \not\equiv 12 \pmod{50}$. Nous verrons les réponses à ces questions à la section suivante PGCD et PPCM.

Soit γ une classe de congruence modulo n, $(n \neq 0)$, et a un élément fixe de γ. Alors par définition $\gamma = \{a + \lambda n\}_{\lambda \in \mathbb{Z}}$.

Proposition 2.7. *Dans chaque classe de congruence γ modulo n, il y a un et un seul élément de $[\![0, n-1]\!]$, autrement dit $\gamma \cap [\![0, n-1]\!]$ est un singleton.*

On désigne par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruence modulo n dans $\mathbb{Z}$. Si $a \in \mathbb{Z}$, la classe $\gamma_n(a)$ est l'ensemble $\{a + \lambda n\}_{\lambda \in \mathbb{Z}}$ noté $a + n\mathbb{Z}$. Si $\gamma \in \mathbb{Z}/n\mathbb{Z}$, l'unique élément de $\gamma \cap [\![0, n-1]\!]$ s'appelle son reste modulo n. De même si $a \in \mathbb{Z}$, l'unique $r \in [\![0, n-1]\!]$ tel que $a \equiv r \pmod{n}$ est appelé son reste modulo n. On déduit immédiatement :

Théorème 2.8. *L'entier $n \geqslant 1$ étant donné, l'application*

$$\gamma_n : [\![0, n-1]\!] \to \mathbb{Z}/n\mathbb{Z}, \quad r \mapsto r + n\mathbb{Z}$$

est bijective. En particulier, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n.

Si $n = 1$, $\mathbb{Z}/n\mathbb{Z}$ est réduit à un singleton, ce qui présente peu d'intérêt.

On utilise souvent des systèmes complets modulo n : par définition , un tel système est une partie E de $\mathbb{Z}$ telle que chaque classe modulo n rencontre E suivant un singleton, i.e telle que l'application $E \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto x + n\mathbb{Z}$ soit bijective. Par exemple, pour tout $a \in \mathbb{Z}$, $[\![a, a+n-1]\!]$ est un système complet, mais on en utilise parfois de plus subtils.

Nous allons voir sur des exemples comment on calcule sur des congruences :

Exemple 12. Démontrer que $2^{2^5} + 1 \equiv 0 \pmod{641}$ (Euler).

Solution. On remarque : $641 = 5 \times 128 + 1 = 1 + 5 \times 2^7$ et aussi $641 = 2^4 + 5^4$.
Donc $5 \times 2^7 \equiv -1 \pmod{641}$ et $5^4 \equiv -2^4 \pmod{641}$. D'après les propriétés élémentaires des congruences iii) on a :

$$\begin{aligned} (5 \times 2^7)^4 &\equiv (-1)^4 \equiv 1 \pmod{641}, \\ 5^4 \times 2^{28} &\equiv 1 \pmod{641} \\ \text{ii) donne } -2^4 \times 2^{28} &\equiv 1 \pmod{641} \end{aligned}$$

d'où le résultat i.e $2^{32} + 1 \equiv 0 \pmod{641}$.

Exemple 13. Montrer que, pour tout $n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2} \equiv 0 \pmod 7$.

Solution. Puisque $3^6 \equiv 1 \pmod 7$ et $2^3 \equiv 1 \pmod 7$, il suffit de raisonner sur la classe de n modulo 3, ce qui ne laisse que 3 cas à examiner d'où le tableau suivant (dont la dernière ligne répond à question posée) :

reste de n	$\pmod 3$	0	1	2
reste de 2^n	$\pmod 7$	1	2	4
reste de 3^{2n}	$\pmod 7$	1	2	4
reste de 2^{n+2}	$\pmod 7$	4	1	2
reste de 3^{2n+1}	$\pmod 7$	3	6	5
reste de $3^{2n+1}+2^{n+2}$	$\pmod 7$	0	0	0

Dans cet exemple on aurait pu remarquer directement que :

$$3^{2n+1} + 2^{n+2} \equiv 3 \times (3^2)^n + 4 \times 2^n \equiv 3 \times 2^n + 4 \times 2^n \equiv 0 \pmod 7.$$

Application aux critères de divisibilité

Proposition 2.9. *Soit $n = \underline{a_m a_{m-1} \dots a_1 a_0}_{10}$. On a alors*

i) $2|n$ *ssi* $a_0 \in \{0,2,4,6,8\}$,

ii) $3|n$ *ssi* $3|(a_0 + a_1 + \cdots + a_m)$,

iii) $4|n$ *ssi* $4|\underline{a_1 a_0}_{10}$,

iv) $5|n$ *ssi* $a_0 = 0$ *ou* $a_0 = 5$,

v) $9|n$ *ssi* $9|(a_0 + \cdots + a_m)$,

vi) $11|n$ *ssi* $11|(a_0 - a_1 + \cdots + (-1)^m a_m)$.

Démonstration. Commençons par écrire que $n = \underline{a_0 + 10a_1 + \cdots + a_m 10^m}_{10}$.

i) Puisque $2|10^k$ pour tout $k \geqslant 1$, $n \equiv a_0 \pmod 2$.
Ainsi $n \equiv 0 \pmod 2$ ssi $a_0 \equiv 0 \pmod 2$, d'où le résultat puisque $a_0 \in \{0,1,2,\dots,9\}$.

ii) Comme $10 \equiv 1 \pmod 3$, on a $10^k \equiv 1 \pmod 3$ pour tout $k \in \mathbb{N}$.
Donc $n \equiv a_0 + \cdots + a_m \pmod 3$ et donc $n \equiv 0 \pmod 3$ ssi $a_0 + \cdots + a_m \equiv 0 \pmod 3$.

iii) Comme $4|100$, $4|10^k$ pour tout $k \geqslant 2$.
Ainsi $n \equiv a_0 + 10a_1 \pmod 4$ et donc $n \equiv 0 \pmod 4$ ssi $\underline{a_1 a_0}_{10} \equiv 0 \pmod 4$.

iv) Comme $5|10$, $5|10^k$ pour tout entier $k \geqslant 1$.
Ainsi $n \equiv a_0 \pmod 5$ et donc $n \equiv 0 \pmod 5$ ssi $a_0 \equiv 0 \pmod 5$ i.e $a_0 = 0$ ou $a_0 = 5$ puisque $a_0 \in \{0,1,\dots,9\}$.

v) Comme $10 \equiv 1 \pmod 9$, $10^k \equiv 1 \pmod 9$ $\forall\, k \in \mathbb{N}$. Ainsi, $n \equiv a_0 + \cdots + a_m \pmod 9$ et donc $n \equiv 0 \pmod 9$ ssi $a_0 + a_1 + \cdots + a_m \equiv 0 \pmod 9$.

vi) Comme $10 \equiv -1 \pmod{11}$, on a $10^k \equiv (-1)^k \pmod{11}$ pour tout k dans $\mathbb{N}$.
Ainsi, $n \equiv a_0 - a_1 + \cdots + (-1)^m a_m \pmod{11}$ et donc $n \equiv 0 \pmod{11}$ ssi $a_0 - a_1 + \cdots + (-1)^m a_m \equiv 0 \pmod{11}$.

□

Exemple 14. 1) L'entier $n = 5445541$ est-il divisible par 3 ?4 ?5 ?11 ?

2) Soit $n = \underline{a_m \dots a_1 a_0}_{10}$ un entier divisible par 11.
Montrer qu'il en est de même pour $n' = \underline{a_0 a_1 \dots a_m}_{10}$.

Solution. 1) n n'est divisible par aucun d'entre eux.
2) $\sum_{k=0} (-1)^k a_k = \sum_{k=0} (-1)^{m-k} a_{m-k}$

2.2 PGCD et PPCM

2.2.1 PGCD de deux entiers relatifs et algorithme d'Euclide

Proposition 2.10. *Soient a et b dans $\mathbb{Z}$.*
Il existe un unique entier naturel m tel que $a\mathbb{Z}+b\mathbb{Z} = m\mathbb{Z}$. Cet entier m est appelé le PGCD, le plus grand diviseur commun de a et b. On le note $m = \text{pgcd}(a,b)$, (ou $\text{gcd}^2(a,b)$) ou bien $m = a \wedge b$ qu'on utilisera dans ce cours. Ainsi,

$$\exists\, (u,v) \in \mathbb{Z}^2, \quad a \wedge b = au + bv.$$

Démonstration. L'ensemble $a\mathbb{Z}+b\mathbb{Z}$ est un idéal de $(\mathbb{Z},+,\times)$ en tant que somme de deux idéaux de $(\mathbb{Z},+,\times)$, d'où l'existence d'un unique entier naturel m tel que $a\mathbb{Z}+b\mathbb{Z} = m\mathbb{Z}$. □

Proposition 2.11. *Soient a et b dans $\mathbb{Z}$. Un entier relatif d est un diviseur commun de a et b ssi $d|a \wedge b$. Autrement dit, $\mathscr{D}_a \cap \mathscr{D}_b = \mathscr{D}_{a\wedge b}$.*

Démonstration. Raisonnons en deux temps.

($\Leftarrow$) Il suffit de prouver que $a \wedge b$ divise a et b. Comme $a\mathbb{Z}+b\mathbb{Z} = (a\wedge b)\mathbb{Z}$ et que $a\mathbb{Z}$ et $b\mathbb{Z}$ sont contenus dans $a\mathbb{Z}+b\mathbb{Z}$, on a $a\mathbb{Z} \subset (a\wedge b)\mathbb{Z}$ et $b\mathbb{Z} \subset (a\wedge b)\mathbb{Z}$, ce qui signifie que $a \wedge b|a$ et $a \wedge b|b$.

($\Rightarrow$) Supposons que d divise a et b. Comme $(a\wedge b)\mathbb{Z} = a\mathbb{Z}+b\mathbb{Z}$, il existe $(u,v) \in \mathbb{Z}^2$ tel que $a \wedge b = au + bv$: d divise donc $a \wedge b$.

□

Exemple 15. Voici quelques calculs de PGCD.
- Pour tout a dans $\mathbb{Z}$, $0 \wedge a = |a|$, en particulier $0 \wedge 0 = 0$.
- Puisque $\mathscr{D}_6 = \{\pm1, \pm2, \pm3, \pm6\}$ et $\mathscr{D}_8 = \{\pm1, \pm2, \pm4, \pm8\}$, on a $6 \wedge 8 = 2$.
- De même, puisque $\mathscr{D}_7 = \{\pm1, \pm7\}$, on a $6 \wedge 7 = 1$ et $8 \wedge 7 = 1$.
- Plus généralement, pour tout entier naturel n, $n \wedge (n+1) = 1$. En effet, un diviseur commun de n et $n+1$ divise nécessairement $n+1-n = 1$, d'où $\mathscr{D}_n \cap \mathscr{D}_{n+1} = \{\pm1\}$.

L'algorithme d'Euclide permet de calculer le PGCD de deux entiers relatifs par divisions euclidiennes successives. Il est fondé sur le lemme suivant.

Lemme 2.12. *Soient q le quotient et r le reste dans la division euclidienne de a par $b \in \mathbb{N}^*$. Alors $a \wedge b = b \wedge r$.*

Démonstration. Soit d un diviseur commun à a et b. Puisque $r = a - bq$, d est un diviseur commun à r et b. Réciproquement, si d est un diviseur commun à r et b, comme $a = bq + r$, d est un diviseur commun à a et b.
On a donc $\mathscr{D}_{a,b} = \mathscr{D}_{b,r}$ et il en résulte bien que $a \wedge b = b \wedge r$ en vertu de la proposition précédente. □

Proposition 2.13 (Algorithme d'Euclide)**.** *Soient a et b deux entiers naturels avec $b \neq 0$. On note $r_0 = a,\ r_1 = b$. Il existe un entier $n_0 \geqslant 2$ pour lequel le reste r_n dans la division euclidienne de r_{n-2} par r_{n-1} est défini pour tout n compris entre 2 et n_0 et $r_{n_0} = 0$. On a alors $a \wedge b = r_{n_0-1}$.*

Démonstration. Les nombres r_0, r_1 et r_2 sont bien définis car $b \neq 0$. Supposons construits les nombres r_0, r_1, ..., r_{n-1} où $n \geqslant 3$. D'après le théorème de la division euclidienne, si $r_{n-1} \neq 0$, on peut effectuer la division euclidienne de r_{n-2} par r_{n-1} dont le reste r_n vérifie $0 \leqslant r_n < r_{n-1}$. On remarque alors qu'il existe nécessairement un plus petit rang n_0 pour lequel $r_{n_0} = 0$ car sinon la suite $(r_n)_{n\in\mathbb{N}^*}$ serait bien définie, à valeurs dans $\mathbb{N}$ et strictement décroissante, ce qui est absurde. D'après le lemme précédent, pour tout entier $1 \leqslant k \leqslant n_0$, $a \wedge b = r_{k-1} \wedge r_k = r_{n_0-1} \wedge r_{n_0} = r_{n_0-1} \wedge 0 = r_{n_0-1}$. □

Méthode : Calcul du PGCD par l'algorithme d'Euclide

On cherche le PGCD de a et b. On peut toujours supposer $b > 0$. On note $r_0 = a$, $r_1 = b$. Il existe un rang n_0 pour lequel, pour tout entier naturel n tel que $\forall\ n_0 \geqslant n \geqslant 2$, r_n le reste dans la division euclidienne de r_{n-2} par r_{n-1} est bien défini, avec $r_{n_0} = 0$. Comme pour tout entier naturel n tel que $2 \leqslant n \leqslant n_0$, $r_{n-2} \wedge r_{n-1} = r_n \wedge r_{n-1}$, on a $a \wedge b = r_{n_0-1} \wedge r_{n_0} = r_{n_0-1} \wedge 0 = r_{n_0-1}$.
$a \wedge b$ **est le dernier reste non nul dans l'algorithme d'Euclide.**

Exemple 16. Calculer $61542 \wedge 6514$.

Solution. Il suffit de poser les divisions successives

$$\begin{aligned}
61542 &= 6514 \times 9 + 2916 \\
6514 &= 2916 \times 2 + 682 \\
2916 &= 682 \times 4 + 188 \\
682 &= 188 \times 3 + 118 \\
188 &= 118 \times 1 + 70 \\
118 &= 70 \times 1 + 48 \\
70 &= 48 \times 1 + 22 \\
48 &= 22 \times 2 + 4 \\
22 &= 4 \times 5 + \boxed{2} \\
4 &= 2 \times 2 + 0
\end{aligned}$$

et comme $4 = 2 \times 2 + 0$, on a $61542 \wedge 6514 = 2$.

Exemple 17.

1) Calculer $424 \wedge 68$ par l'algorithme d'Euclide.
2) Soit $n \in \mathbb{N}^*$. Calculer $(5^n - 1) \wedge (5^{n+1} - 1)$.

Solution.

1) $424 \wedge 68 = 68 \wedge 16 = 16 \wedge 4 = 4$.
2) $(5^{n+1} - 1) \wedge (5^n - 1) = (5^n - 1) \wedge 4 = 4$.

Proposition 2.14. *Soit $d = a \wedge b$ et soit $m \in \mathbb{Z}$, alors*

(i) $\text{pgcd}(a, b+ma) = \text{pgcd}(a,b) = \text{pgcd}(b,-a)$,

(ii) $\text{pgcd}(am,bm) = |m|\,\text{pgcd}(a,b)$, $m \neq 0$.

(iii) $\text{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

(iv) *Soit $g \in \mathbb{Z} \setminus \{0\}$ tel que $g|a$ et $g|b$, alors* $\text{pgcd}\left(\frac{a}{g}, \frac{b}{g}\right) = \frac{1}{|g|}\text{pgcd}(a,b)$.

Démonstration. (i) Soit $g = \text{pgcd}(a, b+ma)$. Puisque $d|a$ et $d|b$, alors $d|b+ma$ et donc $d|g$. Mais aussi, $g|a$ et $g|b$, i.e $g|\text{pgcd}(a,b) = d$. Puisque d et g sont positifs, on conclut que $d = \text{pgcd}(a,b) = \text{pgcd}(a, b+ma) = g$. On procède de la même façon pour montrer que $\text{pgcd}(a,b) = \text{pgcd}(a,-b)$.

(ii) Supposons d'abord $m > 0$. Puisque $d|a$ et $d|b$, alors $dm|am$ et $dm|bm$; Par conséquent, on a $dm|\text{pgcd}(am,bm)$. Il existe donc un entier $k > 0$ tel que

$$\text{pgcd}(am,bm) = dmk \tag{2.2}$$

et alors $dmk|am$ et $dmk|bm$, d'où $dk|a$ et $dk|b$ ou encore $dk|\text{pgcd}(a,b) = d$. Ainsi on obtient que $k = 1$ et, on a

$$\text{pgcd}(am,bm) = dm = m \cdot \text{pgcd}(a,b) = |m|\,\text{pgcd}(a,b).$$

Si $m < 0$, alors $-m = |m| > 0$ et ainsi

$$\text{pgcd}(am,bm) = \text{pgcd}(-am,-bm) = (a|m|, b|m|) = |m|\,\text{pgcd}(a,b).$$

(iii) Il est clair que

$$d = \text{pgcd}(a,b) = \text{pgcd}\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = d \cdot \text{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right)$$

d'où le résultat.

(iv) On a $a = a_1 g$, $b = b_1 g$, d'où

$$\text{pgcd}(a,b) = \text{pgcd}(a_1 g, b_1 g) = |g|\,\text{pgcd}(a_1,b_1) = |g|\,\text{pgcd}\left(\frac{a}{g}, \frac{b}{g}\right)$$

et le résultat suit.

□

Nous avions affirmé à la section précédente que les congruences ne se comportaient pas comme l'égalité, voici le théorème annoncé qui éclaircit la situation.

Théorème 2.15. *Soient $m \in \mathbb{N}$, $x, y \in \mathbb{Z}$, alors :*

(i) *pour $a \neq 0, ax \equiv ay \pmod{m} \iff x \equiv y \left(\text{mod}\,\frac{m}{a \wedge m}\right)$;*

(ii) *si $ax \equiv ay \pmod{m}$ et $a \wedge m = 1$, alors $x \equiv y \pmod{m}$;*

(iii) *$x \equiv y \pmod{m_i}$ pour $i = 1, 2, ..., r \iff x \equiv y \pmod{m_1 \vee \ldots \vee m_r}$.*

Démonstration. (i) ($\Longrightarrow$) Soit $d = a \wedge m$. Alors par hypothèse, il existe un entier $s \in \mathbb{Z}$ tel que $ax - ay = ms$ et ainsi

$$\frac{a}{d}(x-y) = \frac{m}{d}s \quad \text{ou encore} \quad \frac{m}{d}\Big|\frac{a}{d}(x-y).$$

Par ailleurs, on a que $\frac{a}{d} \wedge \frac{m}{d} = 1$, ce qui entraîne que

$$\frac{m}{d}\Big|(x-y),$$

d'où la conclusion.
($\Longleftarrow$) On a $\frac{m}{d}\Big|(x-y)$, ou encore $m|d(x-y)$; c'est pourquoi $m|a(x-y)$ et ainsi $ax \equiv ay \,(\mathrm{mod}\, m)$.
(ii) Ceci est une conséquence immédiate de (i).
(iii) On considère seulement le cas $r = 2$, le résultat général s'obtenant facilement par induction. Puisque $m_1|(a-b)$ et $m_2|(a-b)$, alors $a-b$ est un commun multiple de m_1 et m_2, ce qui signifie que $(m_1 \vee m_2)|(a-b)$. Ce qui met fin à la démonstration du théorème. □

2.2.2 Entiers premiers entre eux et relation de Bézout

Définition 3. a et b sont premiers entre eux lorsque $a \wedge b = 1$, i.e lorsque leurs seuls diviseurs communs dans $\mathbb{Z}$ sont ± 1.

Théorème 2.16 (Bézout)**.** *Deux entiers relatifs a et b sont premiers entre eux ssi il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.*

Démonstration. Procédons en deux étapes.

($\Rightarrow$) Puisque $a \wedge b = 1$, on a $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ et donc $1 \in a\mathbb{Z} + b\mathbb{Z}$, d'où l'existence de $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

($\Leftarrow$) S'il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$, on a $1 \in a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ et donc $a \wedge b|1$. Cela impose que $a \wedge b = 1$ et donc a et b sont premiers entre eux.

□

Une relation du type $au + bv = 1$ (avec u et v dans $\mathbb{Z}$) est appelée *une relation de Bézout pour les entiers premiers entre eux a* et b. On peut facilement obtenir une telle égalité à l'aide de l'algorithme d'Euclide : en notant $r_0 = a$ et $r_1 = b$, r_2 le reste dans la division euclidienne de r_1 par r_0, ..., r_k (resp. q_k) le reste (resp. le quotient) dans la division euclidienne de r_{k-1} par r_{k-2}, ..., et en notant n_0 l'entier où l'algorithme d'Euclide s'arrête, i.e $r_{n_0} = 0$, et on obtient $r_{n_0-1} = a \wedge b = 1$. De plus, $1 = r_{n_0-1} = r_{n_0-2} - q_{n_0-1} r_{n_0-3}$ d'où l'on tire une relation de Bézout $1 = \alpha_{n_0-2} r_{n_0-2} + \beta_{n_0-3} r_{n_0-3}$. Or on a, $r_{n_0-2} = r_{n_0-3} - q_{n_0-2} r_{n_0-4}$ d'où l'on tire une nouvelle relation de Bézout : $1 = \alpha_{n_0-3} r_{n_0-3} + \beta_{n_0-4} r_{n_0-4}$, et ainsi de suite jusqu'à $a = bq_2 + r_2$, d'où l'on tire une relation de Bézout de la forme $1 = \alpha_0 a + \beta_0 b$.

Exemple 18. Montrer que les entiers 157 et 24 sont premiers entre eux et trouver une relation de Bézout les reliant.

Solution. Appliquons l'algorithme d'Euclide.

$$\begin{aligned} 157 &= 24\times 6+13\\ 24 &= 13\times 1+11\\ 13 &= 11\times 1+2\\ 11 &= 2\times 5+1\\ 2 &= 1\times 2+0 \end{aligned}$$

Le dernier reste non nul dans l'algorithme d'Euclide étant 1, les deux nombres sont bien premiers entre eux. On a successivement :

$$\begin{aligned} 1 &= 11-2\times 5 = 11-(13-11)\times 5\\ &= 6\times 11-5\times 13 = 6\times(24-13)-5\times 13\\ &= 6\times 24-11\times 13 = 6\times 24-11\times(157-6\times 24)\\ 1 &= 72\times 24-11\times 157 \end{aligned}$$

Méthode : Obtention d'une relation de Bézout
Effectuer l'algorithme d'Euclide à partir de $r_0 = a$ et $r_1 = b$, $r_{k-2} = q_k r_{k-1} + r_k$ jusqu'au rang n_0 où $r_{n_0} = 0$. Comme $a \wedge b = 1$, on sait que $r_{n_0-1} = 1$. Partir alors de $1 = r_{n_0-3} - q_{n_0-1} r_{n_0-2}$ en utilisant les calculs de l'algorithme d'Euclide afin d'obtenir une relation de Bézout entre r_k et r_{k-1} jusqu'à celle reliant $r_0 = a$ et $r_1 = b$.

Exemple 19.

1) Trouver une relation de Bézout entre 5 et 7.
2) En déduire une relation de Bézout entre 5^2 et 7, puis entre 5 et 7^2 et enfin entre 5^2 et 7^2.
3) Trouver une relation de Bézout entre 21 et 43.
4) Montrer qu'il existe $(u,v) \in \mathbb{Z}^2$ tel que $8u+11v = 7$.

À partir de la relation $r_k = r_{k-2} - q_k r_{k-1}$, on déduit facilement les coefficients de Bézout grâce au théorème suivant qui les définit de manière récurrente.

Théorème 2.17. *Soient a et b des entiers. Alors*

$$a \wedge b = a x_n + b y_n,$$

où x_n et y_n sont les n^e termes des suites définies par :

$$\begin{aligned} x_0 &= 0, \quad x_1 = 1, & x_k &= x_{k-2} - q_k x_{k-1},\\ y_0 &= 1, \quad y_1 = -q_1, & y_k &= y_{k-2} - q_k y_{k-1}, \end{aligned}$$

pour $k = 2, 3, \ldots, n$ et les q_k sont les quotients dans la division de l'algorithme d'Euclide pour trouver (a,b).

Démonstration. Nous montrerons que $r_k = ax_k + by_k$ pour $k = 1, 2, ..., n$. Puisque $r_n = a \wedge b$ alors nous aurons montré que $a \wedge b = ax_n + by_n$.

On utilise le second principe d'induction. Puisque $r_1 = a - bq_1$ alors on pose $x_1 = 1$ et $y_1 = -q_1$ pour obtenir $r_1 = ax_1 + by_1$. De même,

$$r_2 = b - r_1 q_2 = b - (a - bq_1)q_2 = a(-q_2) + b(1 + q_1 q_2).$$

Supposons que $r_j = ax_j + by_j$ pour tout $j = 1, 2, ..., n-1$ alors

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} \\ &= (ax_{n-2} + by_{n-2}) - q_n(ax_{n-1} - by_{n-1}) \\ &= a(x_{n-2} - q_n x_{n-1}) + b(y_{n-2} - q_n y_{n-1}) \\ &= ax_n + by_n. \end{aligned}$$

Ceci termine la démonstration. □

Exemple 20. Calculer le plus grand commun diviseur de $966 \wedge 429$ et exprimer ce nombre comme une combinaison linéaire de 966 et de 429.

Solution. Puisque

$$\begin{aligned} 966 &= 2 \cdot 429 + 108 \\ 429 &= 3 \cdot 108 + 105 \\ 108 &= 1 \cdot 105 + 3 \\ 105 &= 35 \cdot 3, \end{aligned}$$

On a donc, $966 \wedge 429 = 3$. Alors $q_1 = 2$, $q_2 = 3$, $q_3 = 1$ et $q_4 = 35$. En utilisant les suites $\{x_k\}$ et $\{y_k\}$ on obtient le tableau suivant (Méthode de détermination pratique des coefficients de Bézout) :

n	0	1	2	3	4
q_n		2	3	1	35
x_n	0	1	-3	$\boxed{4}$	
y_n	1	-2	7	$\boxed{-9}$	

On conclut que $x = 4$, $y = -9$ et ainsi $3 = 966 \cdot 4 + 429 \cdot (-9)$.

Soient a_1, a_2 et b trois entiers relatifs tels que $b \wedge a_1 = b \wedge a_2 = 1$. Il existe alors un quadruplet (u, v, w, x) tels que $ua_1 + vb = wa_2 + xb = 1$, d'où

$$(ua_1 + vb)(wa_2 + xb) = 1 = (uw)a_1 a_2 + (vwa_2 + xua_1 + xvb)b$$

et donc $b \wedge (a_1 a_2) = 1$. Par une récurrence immédiate, on déduit la généralisation suivante :

Proposition 2.18. *Soient a_1, a_2, ..., a_n et b dans $\mathbb{Z}$ tels que $\forall\ k \leqslant n$, $b \wedge a_k = 1$. Alors : $b \wedge (a_1 \cdots a_k) = 1$.*

Le lemme suivant dit de Gauss, est un résultat élémentaire mais très utile en arithmétique.

Proposition 2.19 (Lemme de Gauss)**.** *Soient $(a, b, c) \in \mathbb{Z}^3$ tel que $a|bc$ et $a \wedge b = 1$. Alors $a|c$.*

Démonstration. Puisque $a|bc$, il existe $a' \in \mathbb{Z}$ tel que $bc = aa'$. Comme $a \wedge b = 1$, il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. On a donc $c = acu + bcv = a(cu + a'v)$ et donc $a|c$. □

On en déduit la généralisation suivante :
Si $a \wedge b_k$ pour tout $k \leqslant n$ et $a|b_1 \cdots b_n c$, alors $a|c$.

Lemme 2.20. *Soient a_1, a_2 et b dans $\mathbb{Z}$ tels que $a_1 \wedge a_2 = 1$, $a_1|b$ et $a_2|b$. Alors $a_1 a_2|b$.*

Démonstration. Comme $a_1|b$, il existe $q_1 \in \mathbb{Z}$ tel que $b = a_1 q_1$. Puisque $a_1 \wedge a_2 = 1$ et $a_2|b$, on déduit du lemme de Gauss que $a_2|q_1$ et donc $a_1 a_2|b$ □

On déduit le résultat suivant par une récurrence évidente sur $m \in \mathbb{N}^*$.

Proposition 2.21. *Soient $a_1, a_2, \ldots, a_m$ et $b \in \mathbb{Z}$ tels que, pour tout $(i,j) \in \mathbb{N}^2$ vérifiant $i \neq j$, $a_i \wedge a_j = 1$ et $a_i|b$. Alors $a_1 a_2 \cdots a_m|b$.*

2.2.3 PGCD d'un nombre fini d'entiers relatifs

Le PGCD définit une loi de composition sur $\mathbb{Z}$ qui est manifestement commutative. Le lemme suivant prouve que cette loi est associative, ce qui ouvrira la porte à une définition par récurrence du PGCD de $n \geqslant 2$ entiers relatifs.

Lemme 2.22. *Pour tous a, b et c dans $\mathbb{Z}$, on a*

$$(a \wedge b) \wedge c = a \wedge (b \wedge c).$$

Démonstration. On sait que $\mathscr{D}_{a,b,c} = \mathscr{D}_a \cap \mathscr{D}_b \cap \mathscr{D}_c$.
Or on a vu que $\mathscr{D}_{a,b} = \mathscr{D}_a \cap \mathscr{D}_b = \mathscr{D}_{a \wedge b}$ et donc $\mathscr{D}_{a,b,c} = \mathscr{D}_{a \wedge b} \cap \mathscr{D}_c = \mathscr{D}_{(a \wedge b) \wedge c}$. Mais également, on a $\mathscr{D}_{a,b,c} = \mathscr{D}_a \cap (\mathscr{D}_b \cap \mathscr{D}_c) = \mathscr{D}_a \cap \mathscr{D}_{b \wedge c} = \mathscr{D}_{a \wedge (b \wedge c)}$. D'où $\mathscr{D}_{a \wedge (b \wedge c)} = \mathscr{D}_{(a \wedge b) \wedge c}$ et donc $a \wedge (b \wedge c) = (a \wedge b) \wedge c$. □

Pour un nombre fini d'entiers relatifs $a_1, a_2, \ldots, a_n$, on peut donc définir sans ambiguïté le PGCD de $a_1, a_2, \ldots a_n$ par $a_1 \wedge a_2 \wedge \cdots \wedge a_n$. On démontre sans peine par récurrence que

$$\mathscr{D}_{a_1, a_2, \ldots, a_n} = \mathscr{D}_{a_1} \cap \mathscr{D}_{a_2} \cap \cdots \cap \mathscr{D}_{a_n}.$$

On peut également montrer par récurrence à partir de la définition du PGCD que

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = (a_1 \wedge a_2 \wedge \cdots \wedge a_n)\mathbb{Z}.$$

Ainsi, il existe $(u_1, \ldots, u_n) \in \mathbb{Z}^n$ tel que

$$a_1 \wedge a_2 \wedge \cdots \wedge a_n = u_1 a_1 + u_2 a_2 + \ldots + u_n a_n.$$

Définition 4. Des entiers relatifs $a_1, a_2, \ldots, a_n$ sont dits *relativement premiers ou premiers entre eux dans leur ensemble* lorsque leurs seuls diviseurs communs sont ± 1, autrement dit $a_1 \wedge a_2 \wedge \cdots \wedge a_n = 1$.

Cette propriété est équivalente à l'existence d'une relation de Bézout

$$u_1 a_1 + u_2 a_2 + \ldots + u_n a_n = 1.$$

On peut obtenir une telle relation de proche en proche.

Exemple 21. Déterminer une relation de Bézout reliant les entiers 6, 10 et 15.

Solution. On a $6 \wedge 10 \wedge 15 = (6 \wedge 10) \wedge 15 = 2 \wedge 15 = 1$. Les trois entiers sont donc premiers entre eux. On a $2 \times 6 - 10 = 2$. Il suffit alors de trouver une relation de Bézout entre 2 et 15 : $15 - 7 \times 2 = 1$. Ainsi

$$15 - 7 \times (2 \times 6 - 10) = 1 = -14 \times 6 + 7 \times 10 + 1 \times 15.$$

Exemple 22. Des entiers premiers entre eux deux à deux sont-ils premiers entre eux ? Étudier la réciproque.

Solution. L'affirmation est vraie mais la réciproque est fausse, il suffit de considérer $2, 3, 4$. $2 \wedge 4 \wedge 3 = 1$. Alors que $2 \wedge 4 = 2$.

2.2.4 PPCM d'un nombre fini d'entiers relatifs

Comme pour le PGCD, nous commencerons avec le cas de deux entiers relatifs le cas de n s'en déduit facilement.

Proposition 2.23. *Soient a et b dans $\mathbb{Z}$. Il existe un unique naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Cet entier m est appelé le PPCM, le plus petit commun multiple de a et b.*
On le note $m = \text{ppcm}(a, b)$ ou $m = a \vee b$ que l'on utilisera dans ce cours.

Démonstration. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est clairement un idéal de l'anneau $(\mathbb{Z}, +, \times)$. D'où l'existence d'un unique entier naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. □

Comme dans le cas du PGCD, la terminologie PPCM signifie deux propriétés : $a \vee b$ est un multiple de a et de b, et il s'agit du plus petit multiple au sens de la relation d'ordre de la divisibilité sur $\mathbb{N}$ des multiples entiers naturels commun à a et b. La proposition suivante résume ces deux propriétés.

Proposition 2.24. *Soient a et b dans $\mathbb{Z}$. Un entier relatif m est un multiple commun de a et b ssi $a \vee b | m$.*

Démonstration. Le résultat découle immédiatement de l'égalité $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$. □

De la connaissance d'un des nombres $a \vee b$ ou $a \wedge b$ découle celle de l'autre. La proposition suivante éclaire les liens entre le PGCD et le PPCM de deux entiers relatifs.

Proposition 2.25. *Pour tous entiers relatifs a et b on a :*

$$(a \vee b)(a \wedge b) = |ab|.$$

Démonstration. Notons $d = a \wedge b$ et $m = a \vee b$. Les cas où $a = 0$ et $b = 0$ étant triviaux, on suppose a et b non nuls. On a $a = da'$ et $b = db'$ avec $(a', b') \in \mathbb{Z}^2$ tel que $a' \wedge b' = 1$.
Puisque $a = da' | m$, il existe $\alpha \in \mathbb{Z}$ tel que $m = da'\alpha$. Comme $b = db' | m = da'\alpha$ et $d \neq 0$, $b' | a'\alpha$. Or, $a' \wedge b' = 1$, donc, d'après le lemme de Gauss, $b' | \alpha$ et il existe $\beta \in \mathbb{Z}$ tel que $\alpha = b'\beta$ d'où $m = da'b'\beta$, i.e $da'b' | m$. Puisque $da'b' = ab' = ba'$ est clairement un multiple commun de a et b, $m | da'b'$ et donc $m = d\,|a'b'|$.
Ainsi, $|ab| = d^2\,|a'b'| = dm = (a \wedge b)(a \vee b)$. □

Le PPCM définit sur $\mathbb{Z}$ une loi de composition commutative et associative, ce qui permet la définition du PPCM de n entiers relatifs $a_1, a_2, \ldots, a_n$ par $a_1 \vee a_2 \vee \cdots \vee a_n$.

Il est facile de prouver le résultat suivant :

$$\left(\forall\ (a,b,c) \in \mathbb{Z}^3\right), \quad ab \vee ac = |a|\,(b \vee c).$$

(A prouver en exo !).

Exemple 23.

1) Justifier que la loi définie sur $\mathbb{Z}^2$ par le PPCM est associative.

2) Existe-il deux entiers relatifs a et b tels que $a \wedge b = 3$ et $a \vee b = 8$?

Solution. 1). Oui
2). Non car le pgcd divise toujours le ppcm.

2.3 Les nombres premiers

Définition 5. Un entier naturel p est dit premier lorsque $p \geqslant 2$ et que ces seuls diviseurs dans $\mathbb{N}$ sont 1 et p. Un nombre entier non premier est dit composé.

Il est théoriquement possible d'ordonner les nombres premiers en suite croissante (2, 3, 5, 7, 11, 13, etc.), une méthode simple est décrite dans la section qui suit :

2.3.1 Le crible d'Ératosthène

Pour établir une table de nombres premiers, on doit examiner chaque nombre naturel n (dans l'ordre croissant) et déterminer s'il est premier ou composé. En fait, aussitôt qu'un nombre entier n possède un diviseur d tel que $1 < d < n$, on l'élimine. Mais ce processus simple (et jusqu'à un certain point «naïf») exige tout de même que l'on vérifie si n est divisible par chacun des nombres d tels que $1 < d < n$ avant de pouvoir conclure qu'il est premier ou non. Or, en réalité, il suffit de vérifier si n est divisible par un nombre premier $p \leqslant \sqrt{n}$. En effet, supposons que n est composé et que tous les nombres premiers p qui divisent n satisfont à la condition

$$\sqrt{n} < p \leqslant n. \tag{2.3}$$

Il s'ensuit que si un certain nombre premier p_0 divise n et satisfait à (2.3), on pourra écrire $n = p_0 n_0$ pour un certain entier $n_0 > 1$. Mais alors, $n_0 | n$ et

$$n_0 = \frac{n}{p_0} < \frac{n}{\sqrt{n}} = \sqrt{n},$$

et on a ainsi trouvé un diviseur de n qui possède au moins un facteur premier inférieur à $\sqrt{n}$, ce qui est une contradiction.

Théorème 2.26 (Test de primalité). *Un nombre entier naturel n est premier si et seulement si il n'est divisible par aucun nombre premier p,* $1 < p \leqslant \sqrt{n}$.

C'est avec cette règle très simple qu'Ératosthène[3] a construit son crible. Plus précisément, supposons que l'on veuille dresser une liste de tous les nombres premiers inférieurs ou égaux à x ; la méthode d'Ératosthène se décrit comme suit. On écrit d'abord sur un tableau tous les nombres naturels de 2 à x. On raye alors tous les multiples propres de 2 (i.e les multiples de 2 qui sont différents de 2), puis tous les multiples propres de 3, puis tous les multiples propres de 5. On observe ainsi que le plus petit nombre supérieur à 5 qui n'est pas rayé est 7. On raye alors tous les multiples propres de 7. Et ainsi de suite. Toutefois, aussitôt que l'on arrive à l'étape où le plus petit nombre qui n'a pas été rayé est supérieur à $\sqrt{x}$, on arrête le processus et on est assuré que tous les nombres non rayés dans la liste sont tous les nombres premiers $\leqslant x$.

Pour illustrer cette méthode, trouvons tous les nombres premiers $\leqslant 40$. Nous écrivons les entiers de 1 à 40 en rangées. En premier, nous rayons tous les multiples propres de 2. Après 2, on trouve l'entier 3 qui n'est pas supprimé, qui est premier, et on raye tous les multiples propres de 3. Ensuite nous rayons les multiples propres de 5. Nous pouvons terminer car $\sqrt{40} < 7$. Ci-dessous, on a les rangées des entiers qui ont été rayés par la méthode du crible.

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~

Alors les nombres premiers plus petits que 40 sont

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37.$$

Cette méthode est extrêmement simple et est encore utilisée aujourd'hui pour dresser, à l'aide d'ordinateurs très rapides, des listes de nombres premiers.

Exemple 24. L'entier 281 n'est pas divisible ni par 2, ni par 3, ni par 5, ni par 7, ni par 11, ni par 13. Il est inutile de diviser par 17 car $17^2 = 289 > 281$. On en déduit alors que le nombre 281 est premier.

2.3.2 L'ensemble $\mathscr{P}$ des nombres premiers

Lemme 2.27. *Tout entier $n \geqslant 2$ admet au moins un diviseur premier.*

Démonstration. Soit $n \geqslant 2$. Notons E l'ensemble des diviseurs de n qui sont des entiers naturels supérieurs ou égaux à 2. Puisque $n \in E$, E est une partie non vide de $\mathbb{N}$. Soit k le plus petit élément de E. Comme $k \in E$, $k|n$. Montrons que k est premier par l'absurde. Si ce n'était pas le cas, k admettrait un diviseur $1 < k' < k$ et on aurait donc $k'|k$ d'où $k' \in E$ et $k' < \inf(E) = k$, ce qui est absurde. □

Proposition 2.28. *L'ensemble $\mathscr{P}$ des nombres premiers est infini.*

Démonstration. Supposons le contraire, c'est-à-dire qu'il existe un nombre fini de nombres premiers, disons $p_1, p_2, \ldots, p_k$. Alors considérons le nombre

$$N = p_1 p_2 \cdots p_k + 1. \tag{2.4}$$

3. (276 – 194 av. J.-C) fut un mathématicien de l'école d'Alexandrie.

Si N est premier, alors on a trouvé un nombre premier plus grand que p_k et on obtient ainsi une contradiction. Par contre, si N est composé, alors N est divisible par un nombre premier et comme les seuls nombres premiers existants sont $p_1, p_2, \ldots, p_k$, alors il existe un indice i, $1 \leqslant i \leqslant k$ tel que $p_i | N$. Mais alors, il découle de (2.4) que $p_i | 1$, ce qui est une contradiction. □

2.3.3 Le théorème fondamental de l'arithmétique (TFA)

Théorème 2.29 (Premier théorème d'Euclide)**.** *Si p est un nombre premier et si $p \,|\, ab$, alors $p \,|\, a$ ou $p \,|\, b$.*

Démonstration. Si $p|a$, alors le résultat est prouvé. Sinon on a $p \not| a$. Puisque les seuls diviseurs de p sont 1 et p, on a que $a \wedge p = 1$. En faisant appel au lemme de Gauss, on obtient $p|b$. □

Corollaire 2.30.

$$p \,|\, a_1\, a_2 \cdots a_r \Longrightarrow p \,|\, a_1 \text{ ou } p \,|\, a_2 \text{ ou } \ldots \text{ ou } p \,|\, a_r.$$

Démonstration. Il suffit de faire un raisonnement par induction et d'utiliser le théorème précédent. □

Corollaire 2.31. *Si $p, q_1, q_2, \ldots, q_r$ sont des nombres premiers et si $p|q_1q_2 \cdots q_r$, alors $p = q_k$ pour un certain k tel que $1 \leqslant k \leqslant r$.*

Démonstration. On utilise le corollaire précédent en tenant compte du fait que si $p|q_k$, alors $p = q_k$. □

Nous voici prêts à démontrer le TFA.

Théorème 2.32 (Théorème fondamental de l'arithmétique (TFA)).
Tout entier naturel $n > 1$ peut s'écrire comme un produit de facteurs premiers, et cette représentation est unique à l'ordre des facteurs premiers près.

Démonstration. Si n est premier, alors la preuve est terminée. Sinon supposons que n n'est pas premier et considérons l'ensemble

$$D = \{d : d|n \text{ et } 1 < d < n\}.$$

Alors, $D \subset \mathbb{N}$ et, puisque n est composé, on a $D \neq \emptyset$. D'après le PBO, D possède un plus petit élément p_1 qui est premier, sans quoi le choix minimal de p_1 serait contredit. On peut donc écrire $n = p_1 n_1$.
Si n_1 est premier, alors la preuve est finie. Sinon n_1 est composé, alors on répète le même argument que ci-dessus et on en déduit l'existence d'un nombre premier p_2 et d'un entier $n_2 < n_1$ tels que $n = p_1 p_2 n_2$.
En poursuivant ainsi, à la k-ième étape, on a

$$n = p_1 p_2 \cdots p_k n_k \quad \text{avec} \quad n_1 > n_2 > \ldots > n_k > 1.$$

Comme les n_i sont des entiers naturels, le processus a une fin et on arrive à une k-ième étape où n_k est premier, i.e $n_k = p_{k+1}$. On a alors

$$n = p_1 p_2 \cdots p_{k+1},$$

ce qui démontre la première partie du théorème.

Supposons maintenant que l'on a pas l'unicité de la représentation, i.e que

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

On simplifie d'abord cette équation en éliminant au besoin les nombres premiers qui apparaissent des deux côtés à la fois. On obtient alors

$$p_{i_1} p_{i_2} \cdots p_{i_\alpha} = q_{j_1} q_{j_2} \cdots q_{j_\beta}, \tag{2.5}$$

où $\alpha \leqslant r$ et $\beta \leqslant s$. Ainsi dans (2.5), tous les p_i sont différents des q_j. Mais ceci est impossible, car d'après (2.5), $p_{i_1} | q_{j_1} q_{j_2} \cdots q_{j_\beta}$ et ainsi, il existe un entier ρ, $1 \leqslant \rho \leqslant \beta$, tel que $p_{i_1} = q_{j_\rho}$, ce qui contredit le fait que tous les p_i sont différents des q_j. Ceci prouve l'unicité de la représentation. □

Il arrive parfois que l'on veuille comparer les factorisations respectives de deux (ou plus) nombres entiers. Dans ce cas, les représentations canoniques correspondantes pourraient comporter des exposants $a_i = 0$, tout simplement dans le but de pouvoir mieux comparer leur factorisation. C'est ainsi qu'on écrira $10 = 2 \cdot 3^0 \cdot 5$ et $6 = 2 \cdot 3 \cdot 5^0$.

Théorème 2.33. *Soit $n = \prod_{i=1}^{r} q_i^{a_i}$, $a_i > 0$ pour chaque i et soit $d > 0$. Alors*

$$d | n \Longleftrightarrow d = \prod_{i=1}^{r} q_i^{b_i},$$

pour certains entiers non-négatifs $b_i \leqslant a_i$, $i = 1, 2, ..., r$.

Démonstration. Soit $d = \prod_{i=1}^{r} q_i^{b_i}$ avec $0 \leqslant b_i \leqslant a_i$, alors

$$n = \prod_{i=1}^{r} q_i^{a_i} n = \prod_{i=1}^{r} q_i^{a_i - b_i + b_i} = \prod_{i=1}^{r} q_i^{a_i - b_i} q_i^{b_i} = \prod_{i=1}^{r} q_i^{a_i - b_i} \prod_{i=1}^{r} q_i^{b_i} = c \cdot d.$$

où $c = \prod_{i=1}^{r} q_i^{a_i - b_i}$ et $c \geqslant 1$. Donc $d | n$, ainsi qu'il le fallait.

Inversement supposons que $d | n$. Alors, il existe un entier c tel que $cd = n$ et on peut former la représentation canonique de d et celle de c. En tenant compte de la remarque ci-dessus, on peut écrire

$$d = \prod_{i=1}^{r} q_i^{d_i}, \quad c = \prod_{i=1}^{r} q_i^{c_i}, \quad c_i \geqslant 0, \text{ et } d_i \geqslant 0.$$

Puisque $cd = n$, on obtient $a_i = c_i + d_i$ et donc $a_i \geqslant d_i$. □

Théorème 2.34. *Si $a = \prod_{i=1}^{r} q_i^{\alpha_i}$ et $b = \prod_{i=1}^{r} q_i^{\beta_i}$, avec $\alpha_i \geqslant 0$ et $\beta_i \geqslant 0$ pour chaque i, sont les représentations standards de a et b, alors*

$$a \wedge b = \prod_{i=1}^{r} q_i^{\min\{\alpha_i, \beta_i\}} \quad \text{et} \quad a \vee b = \prod_{i=1}^{r} q_i^{\max\{\alpha_i, \beta_i\}}.$$

Démonstration. Soit $d = \prod_{i=1}^{r} q_i^{c_i}$ où $c_i = \min\{\alpha_i, \beta_i\}$. Puisque $c_i \leqslant \alpha_i$, et $c_i \leqslant \beta_i$, alors $d|a$ et $d|b$ et ainsi d est un diviseur commun de a et b. Supposons que $g|a$ et $g|b$, alors $|g| = \prod_{i=1}^{r} q_i^{e_i}$ avec $e_i \leqslant \alpha_i$ et $e_i \leqslant \beta_i$ pour chaque i. Puisque c_i est le plus petit des nombres α_i et β_i, il s'ensuit que $e_i \leqslant c_i$ pour chaque i et ainsi que $|g|$ divise d ; d'où $g|d$. Puisque $d > 0$, on a ainsi montré que $d = a \wedge b$. Pour compléter la preuve, on note tout d'abord que

$$\alpha_i + \beta_i - \min\{\alpha_i, \beta_i\} = \max\{\alpha_i, \beta_i\}.$$

Ensuite, en utilisant la propriété $a \vee b = \dfrac{ab}{a \wedge b}$, on obtient facilement le résultat. □

Exemple 25. Soient $a = 43560$ et $b = 58212$, alors nous trouvons

$$a = 2^3 \cdot 3^2 \cdot 5 \cdot 7^0 \cdot 11^2 \quad \text{et} \quad b = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^2 \cdot 11.$$

On obtient

$$a \wedge b = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11 = 396 \quad \text{et} \quad a \vee b = 2^3 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11^2 = 6403320.$$

2.3.4 La p-valuation sur $\mathbb{N}$

Définition 6. Soit $p \in \mathscr{P}$ et $n \in \mathbb{N}^*$. On note $\nu_p(n)$ l'exposant de p dans la décomposition de n en produit de facteurs premiers. Ce nombre est appelé la *p-valuation de n*

Remarque. On notera que $\nu_p(n)$ est le plus grand entier naturel α tel que $p^\alpha | n$.

On déduit du TFA que, pour tout $n \in \mathbb{N}^*$, il n'existe qu'un nombre fini de nombres premiers p tels que $\nu_p(n) \geqslant 1$ et l'on peut écrire

$$n = \prod_{p \in \mathscr{P}} p^{\nu_p(n)}$$

car ce produit ne compte en fait qu'un nombre fini de facteurs différents de 1. Cette écriture a l'avantage d'être intrinsèque : elle évite le recours à l'indice m et aux exposants α_k.

Lemme 2.35.

$$\left(\forall\ (m,n) \in (\mathbb{N}^*)^2\right) \quad m|n \iff \forall\ p \in \mathscr{P}, \nu_p(m) \leqslant \nu_p(n).$$

Démonstration. Voir théorème 2.33 □

Remarque. Il est facile de vérifier la propriété suivante : pour tous entiers m et n de $\mathbb{Z}^*$ et tout $p \in \mathscr{P}$, on a $\nu_p(mn) = \nu_p(m)\nu_p(n)$.

Une conséquence immédiate de ce lemme est la réécriture du PGCD et du PPCM.

Proposition 2.36. *Soient a et b dans $\mathbb{N} \setminus \{0,1\}$. Alors*

$$a \wedge b = \prod_{p \in \mathscr{P}} p^{\min(\nu_p(a), \nu_p(b))} \quad \text{et} \quad a \vee b = \prod_{p \in \mathscr{P}} p^{\max(\nu_p(a), \nu_p(b))}.$$

2.4 L'équation diophantienne du premier degré

Il s'agit de résoudre dans $\mathbb{Z}$ l'équation $ax+by=c$ d'inconnues x et y les entiers a,b et c étant fixés.

Proposition 2.37. *Soient $(a,b)\in\mathbb{Z}^2$ avec $(a,b)\neq(0,0)$ et $c\in\mathbb{Z}$. Alors l'équation $ax+by=c$ admet au moins une solution ssi $a\wedge b\,|\,c$.*

Démonstration. Supposons que l'équation admette une solution (x,y). Comme $a\wedge b$ divise a et b, alors $a\wedge b\,|\,ax+by=c$ d'où le résultat. Réciproquement, supposons que $a\wedge b\,|\,c$. Écrivons $d=a\wedge b$, $a=da'$, $b=db'$ et $c=dc'$ où $a',b',c'\in\mathbb{Z}$. On sait que $a'\wedge b'=1$. Puisque $(a,b)\neq(0,0)$, $d\neq 0$ et l'équation est équivalente à $a'x+b'y=c'$. Comme $a'\wedge b'=1$, il existe $(u,v)\in\mathbb{Z}^2$ tel que $a'u+b'v=1$, donc $a'uc'+b'vc'=c'$ et le couple $(x,y)=(uc',vc')$ est une solution particulière de l'équation $ax+by=c$. □

Remarquons que la connaissance d'une solution particulière notée (x_0,y_0) de l'équation $a'x+b'y=c'$ (voir ci-dessus) permet la détermination de toutes les autres solutions de l'équation. En effet, (x,y) est une solution ssi $a'x+b'y=c'=a'x_0+b'y_0$ i.e $a'(x-x_0)=b'(y_0-y)$. Puisque $a'\wedge b'=1$, cette égalité équivaut d'après le lemme de Gauss, à l'existence de $k\in\mathbb{Z}$ tel que $x-x_0=kb'$ et $y_0-y=ka'$. L'ensemble des solutions est donc

$$\mathscr{S}=\left\{(x_0+kb',y_0-ka')\,:\,k\in\mathbb{Z}\right\}.$$

Méthode : Résolution de l'équation $ax+by=c$

- Si $a\wedge b$ ne divise pas c, l'équation n'admet aucune solution.
- Si $a\wedge b|c$, écrire $d=a\wedge b$, $a=da'$, $b=db'$, $c=dc'$, a', b' et c' dans $\mathbb{Z}$. L'équation est équivalente à $a'x+b'y=c'$.

1. On commence par rechercher une solution particulière (x_0,y_0) en exploitant une relation de Bézout entre a' et b'.
2. Résoudre l'équation en écrivant qu'un couple (x,y) est solution si, et seulement si $a'x+b'y=a'x_0+b'y_0$ i.e $a'(x-x_0)=b'(y_0-y)$. On applique ensuite le lemme de Gauss $(a'\wedge b'=1)$ pour conclure que les solutions sont les couples d'entiers de la forme (x_0+kb',y_0-ka') avec $k\in\mathbb{Z}$.

Exemple 26. Résoudre dans $\mathbb{Z}^2$ l'équation $3x+2y=5$.

Solution. Comme $3\times 1+2\times(-1)=1$, on a $3\times 5+2\times(-5)=5$. Un couple d'entiers est donc solution ssi $3x+2y=3\times 5+2\times(-5)=5$ i.e $3(x-5)=2(-5-y)$. Puisque $3\wedge 2=1$, on déduit du lemme de Gauss que (x,y) est solution ssi il existe un entier k tel que $x-5=2k$ et $-5-y=3k$. L'ensemble des solutions de $3x+2y=5$ est donc $\{(5+2k,-5-3k)\,:\,k\in\mathbb{Z}\}$.

Exemple 27.

1) Résoudre dans $\mathbb{Z}^2$ l'équation $2x-3y=1$.

2) Résoudre dans $\mathbb{Z}^2$ l'équation $2x+3y=2$.

Solution.

1) $d = 2 \wedge (-3) = 1 | 1$, $2 = 1 \times 2$, $-3 = 1 \times (-3)$ et $1 = 1 \times 1$. Dans ce cas-ci l'équation est équivalente à elle-même. Une relation de Bézout entre 2 et -3 est $2 \times 2 + (-3) \times 1 = 1$. Donc une solution particulière de l'équation est $(x_0, y_0) = (2, 1)$. (x, y) est solution ssi $2(x-2) = -3(1-y)$. En appliquant le lemme de Gauss, on conclut que les solutions sont les couples d'entiers de la forme $(2-3k, 1-2k)$, $k \in \mathbb{Z}$.

2) À vous ! $\{(-2-3k, 2+2k) \ : \ k \in \mathbb{Z}\}$

Chapitre 3

Les anneaux $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Dans ce qui suit, nous fixons l'entier $n \geqslant 2$.

Définition 7. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ par la relation d'équivalence «être congru modulo n».

Nous noterons classiquement $\overline{x}$ la classe de congruence modulo n de l'entier naturel x.

Proposition 3.1. *Pour tous entiers relatifs x et y, on pose*

$$\overline{x} + \overline{y} = \overline{x+y} \qquad et \qquad \overline{x} \cdot \overline{y} = \overline{xy}.$$

On définit ainsi sur $\mathbb{Z}/n\mathbb{Z}$ deux lois de composition pour lesquelles $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

Démonstration. Commençons par prouver que ces deux définitions ont un sens. Soient x, x', y et y' dans $\mathbb{Z}$ tels que $\overline{x} = \overline{x}'$ et $\overline{y} = \overline{y}'$. Pour que la définition $\overline{x} + \overline{y} = \overline{x+y}$ ait un sens il s'agit de vérifier [1] que $\overline{x+y} = \overline{x'+y'}$. C'est bien le cas puisque $x \equiv x' \pmod{n}$ et $y \equiv y' \pmod{n}$ implique $x + y \equiv x' + y' \pmod{n}$. De même, le produit $\overline{x} \cdot \overline{y}$ est bien défini puisque $x \equiv x' \pmod{n}$ et $y \equiv y' \pmod{n}$ implique que $xy \equiv x'y' \pmod{n}$. Il reste à vérifier que ces deux lois confèrent à $\mathbb{Z}/n\mathbb{Z}$ une structure d'anneau commutatif (voir cours de structures algébriques). □

L'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre en général. Par exemple $\overline{2} \cdot \overline{2} = \overline{0}$ dans $\mathbb{Z}/4\mathbb{Z}$, alors que $\overline{2} \neq 0$.

Proposition 3.2. *Soit $n \in \mathbb{N}$. Les propriétés suivantes sont équivalentes :*

i) *$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps ;*

ii) *$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est intègre ;*

iii) *n est premier.*

Démonstration. Il nous suffit de démontrer : 1) ⇒ 2) ⇒ 3) ⇒ 1).

1) ⇒ 2). Un corps est toujours intègre car tout élément non nul est inversible donc régulier pour la loi $\times$.

1. Autrement dit, il s'agit de justifier que $\overline{x+y}$ est indépendant des représentants x et y des classes $\overline{x}$ et $\overline{y}$.

2) $\Rightarrow$ 3). Prouvons cette implication par contraposée. Supposons n non premier : il existe alors n_1 et n_2 dans $\{2,3,\dots,n-1\}$ tels que $n = n_1 n_2$. Ainsi, $\overline{n} = \overline{0} = \overline{n_1 n_2}$, mais comme n ne divise ni n_1, ni n_2, $\overline{n_1} \neq \overline{0}$ et $\overline{n_2} \neq \overline{0}$. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ admet donc des diviseurs de zéro et par conséquent n'est pas intègre.

3) $\Rightarrow$ 1). Supposons n premier. Il suffit de prouver que tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible pour $\times$. Soit $k \in \{1,2,\dots,n-1\}$. Puisque n ne divise pas k et que n est premier, $k \wedge n = 1$. Il existe donc $(u,v) \in \mathbb{Z}^2$ tel que $uk + vn = 1$ et donc

$$\overline{uk + vn} = \overline{u} \cdot \overline{k} = \overline{k} \cdot \overline{u} = \overline{1}.$$

La classe $\overline{k}$ est donc inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ et son inverse vaut $(\overline{k})^{-1} = \overline{u}$.

□

On vient de montrer le résultat suivant :

Proposition 3.3. *Soient $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$. La classe $\overline{k}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ ssi $k \wedge n = 1$.*

On déduit de cette caractérisation des inversibles de $\mathbb{Z}/n\mathbb{Z}$ le petit [2] théorème de Fermat.

Théorème 3.4 (Petit théorème de Fermat). *Soient $p \in \mathscr{P}$ et $n \in \mathbb{N}$. Alors*

$$n^p \equiv n \pmod{p}.$$

De plus, si $p \wedge n = 1$, alors $n^{p-1} \equiv 1 \pmod{p}$.

Démonstration. Puisque p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. Ainsi $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ est un groupe d'ordre $p-1$. On a donc pour tout $\alpha \in \mathbb{Z}/p\mathbb{Z}^*$, $\alpha^{p-1} = \overline{1}$ et donc $\alpha^p = \alpha$. Cette dernière égalité est encore valable en $\alpha = 0$. Ainsi, pour tout $n \in \mathbb{N}$, on a $\overline{n}^p = \overline{n}$, i.e $n^p \equiv n \pmod{p}$. Si $p \wedge n = 1$, on sait que $\overline{n} \in \mathbb{Z}/p\mathbb{Z}^*$ et donc $\overline{n}^{p-1} = \overline{1}$, i.e $n^{p-1} \equiv 1 \pmod{p}$. (Ou bien $p | n^p - n = n(n^{p-1} - 1) \Rightarrow p | n^{p-1} - 1 \Rightarrow n^{p-1} \equiv 1 \pmod{p}$) □

3.1 Indicateur d'Euler

Le groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sera dorénavant noté $G(n)$. Son cardinal étant noté $\varphi(n)$. L'entier $\varphi(n)$ s'appelle *l'indicateur d'Euler* de n. On a facilement le théorème suivant

Théorème 3.5. *Soit $\mathscr{E}_n$ l'ensemble des entiers $k \in [\![0, n-1]\!]$ qui sont premiers avec n ; l'application $k \mapsto \overline{k}$ définit une bijection de $\mathscr{E}_n$ sur le groupe $G(n)$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. En particulier*

$$\varphi(n) = \mathrm{card}(\mathscr{E}_n).$$

2. Le grand théorème de Fermat affirme que l'équation $x^n + y^n = z^n$ n'admet aucune autre solution entière pour $n \geqslant 3$ que les solutions évidentes pour lesquelles $xyz = 0$. Le mathématicien Andrew Wiles a démontré ce théorème en 1994, après 10 années de recherche solitaires et presque secrètes, mais aussi dans le prolongement de quatre siècles d'efforts de nombreux mathématiciens.

Par convention, on pose $\varphi(1) = 1$ car dans ce cas, $G(1)$ est un singleton. On prouve en passant que

$$\text{card}(\mathscr{E}_{mn}) = \text{card}(\mathscr{E}_m)\,\text{card}(\mathscr{E}_n).$$

La fonction φ d'Euler possède comme un certain nombre d'autres fonctions arithmétiques, la propriété d'être une *fonction multiplicative* : ce qui se traduit par :

Propriété : φ est multiplicative
Soient m et n deux entiers premiers entre eux $(m \geqslant 2, n \geqslant 2)$. Alors on a $\varphi(mn) = \varphi(m)\varphi(n)$.

Théorème 3.6 (Théorème d'Euler). *Soit n un entier naturel $\geqslant 2$, et soit a un entier premier avec n. Alors*

$$\boxed{a^{\varphi(n)} \equiv 1 \pmod{n}}.$$

Démonstration. En exo. □

Remarque. Soient a et n premiers entre eux dans $\mathbb{Z}$.
Par définition, **la période de** $a \pmod{n}$ est l'ordre de $\overline{a}$ du groupe $G(n)$. Soit d cet ordre : il est tel que $\overline{a}^d = \overline{1}$ et que l'ensemble des $k \in \mathbb{Z}$ tel que $\overline{a}^k = \overline{1}$ est $d\mathbb{Z}$.
Le théorème d'Euler signifie donc que **la période de** $a \pmod{n}$ **est un diviseur de** $\varphi(n)$.

Une interprétation du théorème de Fermat nous conduit à un critère de primalité : le théorème de Wilson :

Théorème 3.7 (Théorème de Wilson). *Soit p un entier $\geqslant 2$. Pour que p soit premier, il faut et il suffit que :* $(p-1)! + 1 \equiv 0 \pmod{p}$.

Démonstration. ($\Longrightarrow$) Soit $m = p$ un nombre premier. Si $p = 2$ ou 3, la conclusion est facilement vérifiée. Supposons $p \geqslant 5$ et considérons les entiers r tels que $1 \leqslant r \leqslant p-1$. Il est clair qu'on a toujours $(r, p) = 1$. Et pour chaque $1 \leqslant r \leqslant p-1$, il existe un entier m $(1 \leqslant m \leqslant p-1)$ tel que $mr \equiv 1 \,(\text{mod}\, p)$. Comme $mr \equiv rm \equiv 1 \,(\text{mod}\, p)$, il est clair que si r est associé à m alors m est aussi l'entier associé à r. À l'entier $r = 1$, est évidemment associé l'entier $m = 1$; de même $p-1$ est associé à lui-même. Soit r tel que $2 \leqslant r \leqslant p-2$. Aucun de ces entiers r n'est associé à lui-même, car autrement on aurait $r^2 \equiv 1 \,(\text{mod}\, p)$, i.e $(r-1)(r+1) \equiv 0 \,(\text{mod}\, p)$, ce qui n'est pas possible, puisque $(r-1, p) = (r+1, p) = 1$ pour chaque $2 \leqslant r \leqslant p-2$. Il s'ensuit donc que les entiers 2, 3, ..., $p-3$, $p-2$ peuvent être arrangés en des couples (r, m) tels que $r \neq m$ et $rm \equiv 1 \,(\text{mod}\, p)$. Or, comme $p-1 \equiv -1 \,(\text{mod}\, p)$, il s'ensuit que

$$(p-1)! = 1 \cdot 2 \cdots (p-2)(p-1) \equiv 1 \cdot (p-1) \equiv -1 \,(\text{mod}\, p),$$

d'où la conclusion.
($\Longleftarrow$) Si m n'est pas premier, $m = a \cdot b,\ 1 < a < m$, et alors $a | (m-1)!$. On obtient donc que $a \not| ((m-1)! + 1)$ et, a fortiori, $m \not| (m-1)! + 1)$, ce qui complète la démonstration. □

Exemple 28.

D'après le théorème de Fermat, le nombre $10^6 - 1$ est divisible par 7. Il est facile de le vérifier en divisant 999 999 par 7.

D'après le théorème de Wilson, le nombre $10! + 1$ est divisible par 11. On peut le vérifier en utilisant un critère de divisibilité par 11.

Remarque. La réciproque du théorème de Fermat est fausse. Par exemple, $341|2^{341}-2$ et pourtant $341 = 11 \times 31$ donc pas premier.

Soit α un entier $\geqslant 1$ et soit p un nombre premier ; les nombres k, éléments de $[\![1, p^\alpha - 1]\!]$ qui sont premiers avec p^α sont ceux sont non divisibles par p. Or les nombres divisibles par p dans $[\![1, p^\alpha - 1]\!]$ sont les multiples de p : $p, 2p, \ldots, qp$ où $q = p^{\alpha-1} - 1$; ils sont au nombre de $p^{\alpha-1} - 1$; donc le nombre des $k \in [\![1, p^\alpha - 1]\!]$ qui sont premiers avec p est égal à

$$p^\alpha - 1 - (p^{\alpha-1} - 1) = p^\alpha - p^{\alpha-1}.$$

Ce nombre est l'indicateur d'Euler de p^α. On a donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

Si n est premier, il est clair que : $\varphi(n) = n - 1$.
Si n n'est pas pas premier, on peut calculer $\varphi(n)$, si l'on connaît les facteurs premiers p de n (que l'on notera $p \in \mathscr{P}(n)$), grâce à la relation suivante :

$$\boxed{\varphi(n) = n \prod_{p \in \mathscr{P}(n)} \left(1 - \frac{1}{p}\right)}$$

Exemple 29. Avec $a = 999\,999 = 3^3 \times 7 \times 11 \times 13 \times 37$, on obtient

$$\varphi(a) = a \times \frac{2}{3} \times \frac{6}{7} \times \frac{10}{11} \times \frac{12}{13} \times \frac{36}{37} = 466\,560.$$

3.2 Les congruences linéaires

Les applications intéressantes des congruences aux problèmes de divisibilité nous conduisent à résoudre des congruences contenant des inconnues. Par exemple, si nous voulons trouver tous les entiers positifs n tels que n et n^3 aient les deux derniers chiffres identiques, alors nous devons résoudre la congruence $n^3 \equiv n \pmod{100}$. Dans cette section, pour une variable inconnue x, nous trouverons les valeurs de x vérifiant la congruence linéaire $ax \equiv b \pmod{m}$. Dans le système des nombres rationnels, pour résoudre $ax = b$, nous divisons par a ou de façon équivalente nous multiplions les deux membres de l'équation par l'inverse multiplicatif de a. Nous appliquerons pratiquement le même procédé pour les congruences.

Remarque. Nous noterons l'inverse de a modulo m par $a^{-1} \pmod{m}$

Théorème 3.8. *Un entier a est inversible modulo m si et seulement si $a \wedge m = 1$. Si a possède un inverse, alors il est unique modulo m.*

Exemple 30. Trouver l'inverse de 15 modulo 53.
SOLUTION.
En appliquant l'algorithme d'Euclide aux entiers 15 et 53 nous trouvons

$$2 \cdot 53 - 7 \cdot 15 = 1.$$

Alors $-7 \cdot 15 \equiv 1 \pmod{53}$ et ainsi -7 est un inverse de 15 modulo 53. Puisque $-7 \equiv 46 \pmod{53}$, alors 46 est aussi un inverse de 15 modulo 53.

Nous abordons maintenant la solution d'une congruence linéaire. Pour résoudre $ax \equiv b \pmod{m}$, nous multiplions cette équation par $a^{-1} \pmod{m}$ si a est inversible. Dans ce cas, nous obtenons $x \equiv a^{-1}b \pmod{m}$ qui est la solution.

Exemple 31. Trouver la solution de $17x \equiv 8 \pmod{33}$.
SOLUTION.
L'inverse de 17 modulo 33 est 2. Par conséquent, nous avons la solution $x \equiv 16 \pmod{33}$.

Soit $P(x)$ un polynôme dont les coefficients sont dans $\mathbb{Z}$. Un entier x satisfaisant $P(x) \equiv 0 \pmod{m}$ est appelé *solution* de la congruence. Or si $x \equiv y \pmod{m}$, on a $P(x) \equiv P(y) \pmod{m}$ et alors toute congruence possédant une solution, en possède une infinité. On adoptera donc la convention que les solutions de la congruence sont les solutions «non congrues».

Théorème 3.9. *La* congruence $ax \equiv b \pmod{m}$ *possède exactement une solution si* $a \wedge m = 1$. *Plus généralement, si* $d = a \wedge m$, *alors*

$$ax \equiv b \pmod{m}$$

possède au moins une solution si et seulement si $d|b$, *auquel cas elle possède exactement* d *solutions, lesquelles sont données par*

$$x \equiv x_0 + \frac{km}{d} \pmod{m}, \quad k = 0, 1, 2, \ldots, d-1,$$

où x_0 *est une solution particulière de la congruence* $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

Démonstration. **Cas** 1 Si $a \wedge m = 1$, alors a est inversible et donc la congruence possède une solution x_0.
Si $x = x^*$ est une autre solution de $ax \equiv b \pmod{m}$, alors on a

$$ax^* - ax_0 \equiv b - b \equiv 0 \pmod{m},$$

et donc $a(x^* - x_0) \equiv 0 \pmod{m}$, ce qui veut dire que $x^* \equiv x_0 \pmod{m}$. C'est pourquoi la solution $x = x_0$ est la solution unique modulo m de $ax \equiv b \pmod{m}$. Ainsi toutes les solutions sont données par $x = x_0 + jm$, où $j = 0, \pm 1, \pm 2, \ldots$.

Cas 2 Si $a \wedge m = d > 1$, on procède comme suit. Supposons d'abord que $d \nmid b$. Alors, comme $d|a$, on a que $d \nmid (ax - b)$, pour tout entier x. Cela entraîne que $m \nmid (ax - b)$, i.e que $ax \not\equiv b \pmod{m}$. Supposons maintenant que $d|b$, alors $ax \equiv b \pmod{m}$ est résoluble si et seulement si on peut trouver un entier x tel que $m|(ax - b)$. Or $d|m$, $d|a$, $d|b$ veut dire que

$$ax \equiv b \pmod{m} \Longleftrightarrow (\star) \quad \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

Comme $a/d \wedge m/d = 1$, on est ramené au cas 1 et on peut conclure qu'il existe une solution unique x_0 modulo m/d. Cela signifie que toutes les solutions de $(\star)$ et donc celles de $ax \equiv b \pmod{m}$ sont données par

$$x = x_0 + j\frac{m}{d}, \quad j = 0, \pm 1, \pm 2, \ldots, .$$

C'est ainsi que l'on constate aisément qu'il y a d solutions distinctes modulo m de $ax \equiv b \pmod{m}$.

□

Exemple 32. Montrer que la congruence $34x \equiv 60 \pmod{98}$ possède deux solutions, tandis que la congruence $12x \equiv 9 \pmod{6}$ n'a pas de solution. SOLUTION.
Puisque $34 \wedge 98 = 2$ et $2|60$, la congruence a deux solutions. Nous avons $8 \cdot 49 - 23 \cdot 17 = 1$ ou encore $8 \cdot 98 - 23 \cdot 34 = 2$ et ainsi l'inverse de 17 modulo 49 est -23 ou encore 26. Donc trouver la solution de $34x \equiv 60 \pmod{98}$ revient à trouver la solution de

$$17x \equiv 30 \pmod{49}.$$

La solution de cette dernière congruence est donnée par

$$x = 30 \cdot 26 \equiv 45 \pmod{49},$$

on en conclut que les deux solutions sont $x \equiv 45,\ 94 \pmod{98}$.

Puisque $12 \wedge 6 \not| 9$, la seconde congruence ne possède pas de solution.

3.3 Le théorème du reste chinois

On démontre dans cette section un théorème qui s'avère très important dans la résolution de systèmes de congruences linéaires.

Théorème 3.10. *Soient $m_1, m_2, \ldots, m_r$ des nombres naturels relativement premiers deux à deux. Soient $a_1, a_2, \ldots, a_r$ des entiers quelconques. Alors le système de congruences*

$$\begin{cases} x & \equiv & a_1 & (\mathrm{mod}\, m_1) \\ x & \equiv & a_2 & (\mathrm{mod}\, m_2) \\ & \vdots & & \\ x & \equiv & a_r & (\mathrm{mod}\, m_r) \end{cases}$$

possède une solution x_0 définie ci-après. De plus toutes les solutions sont congrues modulo $m_1 m_2 \cdots m_r$.

Démonstration. Posons $m = m_1 m_2 \cdots m_r$. Il est clair que $m_j \wedge (m/m_j) = 1$ pour tout j. Donc d'après le théorème 3.9, il existe des entiers b_j tels que $(m/m_j) \cdot b_j \equiv 1 (\mathrm{mod}\, m_j)$. Par ailleurs, il est évident que si $i \neq j$ alors $(m/m_j) \cdot b_j \equiv 0 (\mathrm{mod}\, m_i)$. On prétend que la solution du système est donnée par

$$x_0 = \sum_{j=1}^{r} \frac{m}{m_j} \cdot b_j a_j. \tag{3.1}$$

En effet, on a, pour chaque $i = 1, 2, ..., r$,

$$x_0 = \sum_{j=1}^{r} \frac{m}{m_j} \cdot b_j a_j \equiv \frac{m}{m_i} \cdot b_i a_i \equiv a_i (\mathrm{mod}\, m_i).$$

Il reste à prouver l'unicité. Soient x_1 et x_2 deux solutions du système, alors $x_1 \equiv x_2 (\mathrm{mod}\, m_i)$ pour $i = 1, 2, ..., r$ et ainsi $x_1 \equiv x_2 (\mathrm{mod}\, m)$. □

Exemple 33. Trouver le plus petit entier positif x tel que

$$\begin{cases} x & \equiv & 2 & (\mathrm{mod}\, 3), \\ x & \equiv & 3 & (\mathrm{mod}\, 5), \\ x & \equiv & 4 & (\mathrm{mod}\, 7). \end{cases}$$

SOLUTION.
On a $m_1 = 3$, $m_2 = 5$, $m_3 = 7$ et $m = 105$. Puisque l'énoncé

$$(m/m_j) \cdot b_j \equiv 1 \pmod{m_j}, \quad j = 1,2,3,$$

donne les valeurs $b_1 = 2$, $b_2 = 1$, $b_3 = 1$, la solution cherchée est

$$x_0 = \sum_{j=1}^{3} \frac{m}{m_j} \cdot b_j a_j = 263 \equiv 53 \pmod{105}.$$

Une autre façon élégante de procéder est la suivante. La première équation permet d'écrire $x = 2 + 3t$ et en remplaçant dans la seconde, on obtient $2 + 3t \equiv 3 \pmod{5}$ et alors $t \equiv 2 \pmod{5}$. Donc $x = 8 + 15u$ et, en substituant cette valeur dans la troisième équation, on obtient $u \equiv 3 \pmod{7}$ et finalement $x \equiv 53 \pmod{105}$.

Exemple 34. Trouver le plus petit entier positif x tel que

$$\begin{cases} x \equiv 3 \pmod{8}, \\ x \equiv 11 \pmod{20}. \end{cases}$$

SOLUTION.
Nous remarquons que les entiers 8 et 20 ne sont pas relativement premiers et donc nous ne pouvons appliquer le théorème du reste chinois sous sa forme. Pour ce faire, nous pouvons procéder comme suit. Puisque 20 n'est pas une puissance d'un nombre premier, on remplace la seconde congruence par les deux congruences

$$x \equiv 11 \pmod{4}, \qquad x \equiv 11 \pmod{5}.$$

Dans ce cas, on a les trois congruences suivantes :

$$\begin{aligned} x &\equiv 3 \pmod{8}, \\ x &\equiv 3 \pmod{4}, \\ x &\equiv 1 \pmod{5}. \end{aligned}$$

Mais $x \equiv 3 \pmod{8}$ implique $x \equiv 3 \pmod{4}$, alors $x \equiv 3 \pmod{4}$ n'est pas nécessaire. Donc il suffit de résoudre

$$\begin{cases} x \equiv 3 \pmod{8}, \\ x \equiv 1 \pmod{5} \end{cases}$$

et nous remarquons que les entiers 5 et 8 sont relativement premiers. En utilisant le théorème du reste chinois, nous obtenons la solution $x \equiv 11 \pmod{40}$ et ainsi la plus petite solution positive est $x = 11$.

Chapitre 4

Les nombres rationnels

Introduction

Dans $\mathbb{Z}$, il n'est pas toujours possible de définir l'opération inverse de la multiplication. On se propose de rendre cette opération toujours possible, par une **extension convenable de** $\mathbb{Z}$.

Dans le cas de deux entiers naturels a et b, tels que $a = b \cdot q$, on a $ac = bc \cdot q$ pour tout $c \in \mathbb{N}^*$. Ainsi $q = a : b$ peut, d'une infinité de manières s'écrire sous forme d'un quotient de deux entiers.

Exemple 35.

$$2 = 6 : 3 = 12 : 6 = 18 : 9 = 24 : 12, \text{ etc.}$$

Tous les couples $(6,3),(12,6),(18,9),(24,12)$ définissent le même quotient. À partir de cette remarque et par un procédé analogue à celui utilisé pour la construction de l'anneau $\mathbb{Z}$, on va **construire** l'extension projetée.

4.1 L'ensemble $\mathbb{Q}$ des fractions

Soit $\mathscr{Q}$ la relation définie ainsi : deux couples (a,b) et (a',b') sont en relation par $\mathscr{Q}$, $(a,b)\mathscr{Q}(a',b')$ ssi $ab' = a'b$ et $bb' \neq 0$. $\mathscr{Q}$ est une relation d'équivalence dans l'ensembles des couples d'entiers relatifs, à deuxième composante non nulle.

En effet, cette relation est

1. réflexive (à vérifier !)
2. symétrique (à vérifier !)
3. transitive (à vérifier !)

Une classe d'équivalence contient donc tous les couples qui sont en relation par $\mathscr{Q}$ avec l'un quelconque d'entre eux choisi comme représentant de la classe. Rappelons que tout couple appartient à une seule classe.
L'ensemble de toutes les classes est **désigné par** $\mathbb{Q}$. Une classe est dite **fraction**, le premier terme d'un de ses représentants est le **numérateur**, le second le **dénominateur**.
Notation : $(a,b) = \dfrac{a}{b}$ avec $b \neq 0$. On dit aussi (et plus souvent d'ailleurs) **«nombre rationnel»** au lieu de fraction.

4.2 Propriétés de $\mathbb{Q}$

Soient $a, b \in \mathbb{Z}$ et supposons qu'il existe $q \in \mathbb{Z}$ tel que $a = bq$; on a :

$$(a,b)\mathscr{Q}(q,1).$$

Or l'application $(q,1) \mapsto q$ est une bijection de l'ensemble des couples d'entiers dont la première composante est un entier relatif et la seconde 1 ; il est donc légitime d'écrire plus brièvement :

$$q\mathscr{Q}(a,b).$$

Réciproquement, tout entier relatif q peut être considéré comme une fraction de dénominateur 1 : $q\mathscr{Q}(q,1)$.

Ainsi, pour les couples (a,b) tels que a soit divisible par b, la relation $\mathscr{Q}$ n'est autre que la relation d'égalité et les entiers relatifs des représentants des diverses classes de tels couples. Donc $\mathbb{Z} \subset \mathbb{Q}$ et il est légitime de remplacer la notation $\mathscr{Q}$ par le signe "=" s'appliquant dans $\mathbb{Z}$.

Si $\quad a = b, \quad (a,a) = (a:a,1) = (1,1) = 1$
Si $\quad b = aq, \quad (a,b) = (a,aq) = (1,q).$

La fraction ainsi obtenue est dite alors **«inverse»** de l'entier relatif q.

4.2.1 Écriture conventionnelle des fractions

Quand les deux termes d'une fraction son numériques (par exemple $\dfrac{(+5)}{(-3)}$) ; il est commode d'utiliser une autre notation ; on remarque en effet que :

$$\frac{a}{b} = (a,b) = (ab,b^2) = \frac{ab}{b^2}.$$

On peut ainsi supposer que le dénominateur est positif ($\in \mathbb{N}^*$), le numérateur ayant le signe du produit ab qui s'obtient à l'aide de la règle des signes. D'où la règle suivante :

RÈGLE 5. La fraction $\dfrac{a}{b}$ s'écrit $\pm\dfrac{|a|}{|b|}$, le signe étant $+$ ou $-$ suivant que a et b soient ou non de même signe.

$\dfrac{|a|}{|b|}$ est dite valeur absolue de la fraction.

4.2.2 Addition de deux fractions

Définissons une **loi de composition sur** $\mathbb{Q}$ qui à deux fractions $\dfrac{a}{b}$ et $\dfrac{c}{d}$ fait correspondre une troisième fraction dite «somme» des deux autres par l'égalité :

$$\boxed{\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad (bd \neq 0)}.$$

i) Cette loi est **compatible avec la notion de classes de couples**, i.e que l'égalité précédente subsiste quand on remplace par exemple : $\frac{a}{b}$ par $\frac{a'}{b'} = \frac{a}{b}$.
En effet, on a successivement :

$$ab' = a'b,$$

d'où en multipliant par d :

$$adb' = a'db$$

puis en ajoutant bcb' :

$$adb' + bcb' = a'db + bcb'$$

et en mettant b' en facteur et b en facteur de l'autre côté, puis en multipliant par d :

$$(ad+bc)b'd = (a'd+b'c)bd \quad \text{ou} \quad \frac{ad+bc}{bd} = \frac{a'd+b'c}{b'd}.$$

ii) Cette loi est **commutative**. En effet,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{bd} = \frac{c}{d} + \frac{a}{b}.$$

iii) Il existe un élément neutre unique pour cette loi :

$$(0,1) = \frac{0}{1} = 0$$

tel que $\frac{a}{b} + 0 = \frac{a}{b}$. En effet, pour que

$$\frac{a}{b} + \frac{x}{y} = \frac{a}{b},$$

il faut et il suffit que :

$$\frac{ay+bx}{by} = \frac{a}{b} \quad \text{ou} \quad aby + b^2x = aby \quad \text{ou} \quad b^2x = 0 \Rightarrow x = 0.$$

Une fraction de numérateur nul est nulle.

iv) L'opération inverse de l'addition ou **soustraction** consiste à déterminer une fraction $\frac{x}{y}$ telle que $\frac{c}{d} + \frac{x}{y} = \frac{a}{b}$, $\frac{a}{b}$ et $\frac{c}{d}$ étant des fractions données.
On vérifie facilement qu'on a $\frac{x}{y} = \frac{ad-bc}{bd}$. Remarquons que la soustraction $ad-bc$ est toujours possible. On notera $\frac{x}{y} = \frac{a}{b} - \frac{c}{d}$, $\frac{x}{y}$ est la différence. En particulier, si $a = 0$, $\frac{x}{y} = -\frac{c}{d}$, $\frac{x}{y}$ est dite opposée de $\frac{c}{d}$. On l'obtient donc en remplaçant dans $\frac{c}{d}$ le numérateur par son opposé.

RÈGLE 6. Pour retrancher une fraction d'une autre fraction, on ajoute à ce dernier l'opposé du permier.

Théorème 4.1. *L'addition est une **loi de groupe abélien** sur $\mathbb{Q}$, car elle est partout définie, associative et commutative, admet un neutre (0) et tout élément de $\mathbb{Q}$ admet un opposé.*

Remarque. Désormais une somme de fractions s'écrira sans indiquer de parenthèses.

4.2.3 Multiplication des fractions

Définition 8. À une paire quelconque de fractions $\left\{\frac{a}{b}, \frac{c}{d}\right\}$, faisons correspondre une troisième fraction, dite «**produit**», par l'égalité

$$\boxed{\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}}.$$

On définit ainsi sur $\mathbb{Q}$ une loi de composition dite «**multiplication**».

Propriétés :

i) Cette loi est compatible avec l'équivalence définie sur $\mathbb{Q}$; en effet, remplaçons le couple (a,b) par un équivalent (a',b') ; on a : $a'b = ab'$ et en multipliant par cd, il vient :

$$ab'cd = abcd \qquad \text{ou encore} \quad ac(b'd) = bd(a'c)$$

égalité exprimant l'égalité des fractions $\frac{ac}{bd}$ et $\frac{a'c}{b'd}$.

ii) Cette loi est **commutative**, car $\frac{a}{b} \times \frac{c}{d} = \frac{ca}{db} = \frac{c}{d} \times \frac{a}{b}$ et associative, car, étant donné trois fractions, on a :

$$\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right).$$

En même temps, on constate que le produit de plusieurs fractions est une fraction dont le numérateur et le dénominateur sont respectivement les produits des numérateurs et dénominateurs des fractions.
Signalons qu'en particulier on convient de noter $\left(\frac{a}{b}\right)^n$ le produit de n fractions égales $(n \in \mathbb{N})$ et de le nommer «puissance n-ième de la fraction $\frac{a}{b}$». On a :

$$\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}.$$

iii) Il existe pour cette loi un élément neutre unique : la fraction $\frac{1}{1} = 1$, car on a $\frac{a}{b} \cdot \frac{x}{y} = \frac{a}{b}$ ssi $abx = aby$, i.e $x = y$. Or $\frac{x}{x} = \frac{1}{1} = 1$.

iv) L'opération inverse de la multiplication consistera à déterminer une fraction $\frac{x}{y}$ qui multipliée par une fraction donnée $\frac{c}{d}$ permet d'obtenir une fraction $\frac{a}{b}$ également donnée.
La fraction $\frac{x}{y}$ est donc telle que $\frac{c}{d} \cdot \frac{x}{y} = \frac{a}{b}$ et on l'appelle quotient de $\frac{a}{b}$ par $\frac{c}{d}$.
x et y sont donc tels que :

$$\frac{cx}{dy} = \frac{a}{b} \qquad \text{ou} \qquad bcx = ady.$$

Ainsi,

$$\frac{x}{y} = \frac{ad}{bc} = \frac{a}{b} \cdot \frac{d}{c}$$

(Si $bc \neq 0$, donc si $c \neq 0$ puisque $b \neq 0$ à priori). Ainsi la division est toujours possible si le diviseur n'est pas nul.

RÈGLE 7. Le quotient s'obtient en multipliant la fraction dividende par la fraction diviseur «renversée».

En résumé, i), ii), iii) et iv) montrent que la multiplication est une loi de groupe sur $\mathbb{Q}\setminus\{0\}$.

Il est facile de vérifier que la multiplication est **distributive par rapport à l'addition** :

$$\frac{a}{b}\cdot\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}.$$

4.2.4 Structure de corps de $\mathbb{Q}$

En résumé, on a défini deux lois de groupe abéliens ; l'une sur $\mathbb{Q}$, l'**addition**, et l'autre sur $\mathbb{Q}\setminus\{0\}$, la **multiplication**. La seconde est distributive par rapport à la première. Ces deux lois déterminent sur $\mathbb{Q}$ une structure de **corps commutatif** et on sous-entendra l'existence d'une telle structure, quand on emploiera le terme corps des **nombres rationnels**.

4.2.5 Calculs dans $\mathbb{Q}$

Définition 9. Une fraction est dite **irréductible**, ou réduite à sa plus simple expression quand on ne peut plus la simplifier.

Théorème 4.2. *La condition nécessaire et suffisante pour qu'une fraction soit **irréductible** est que ses deux termes soient premiers entre eux.*

Théorème 4.3. *On **réduit une fraction** à sa plus simple expression en divisant ses deux termes par leur **PGCD**.*

Exemple 36.

$$\frac{432}{600}=\frac{24\times 18}{24\times 25}=\frac{18}{25}.$$

Théorème 4.4. *Pour **réduire des fractions au même dénominateur**, on détermine un multiple commun des dénominateurs (en général le PPCM) : on le divise séparément par chacun de ces dénominateurs, puis on multiplie les deux termes de chacune des fractions respectivement par chacun des quotients obtenus.*

Exemple 37. Soient les fractions : $\frac{3}{16}$, $\frac{9}{15}$, $\frac{7}{24}$.

Solution. Le PPCM de 16, 15, 24 est 240.

$$\begin{aligned}\frac{3}{16}&=\frac{3\times 15}{240}=\frac{45}{240}\\ \frac{9}{15}&=\frac{9\times 16}{240}=\frac{144}{240}\\ \frac{7}{24}&=\frac{7\times 10}{240}=\frac{70}{240}.\end{aligned}$$

RÈGLE 8. La **somme** (resp. **différence**) de deux fractions de même dénominateur est une fraction ayant pour dénominateur le dénominateur commun, pour numérateur la somme (resp. différence) des numérateurs.

Pour effectuer la somme (resp. différence) de deux fractions qui n'ont pas même dénominateur, on commencera par les réduire au même dénominateur à l'aide du théorème précédent.

RÈGLE 9. Après réduction à un même dénominateur positif, la **comparaison des fractions** revient à celle des numérateurs et les théorèmes sur les inégalités valables pour les entiers relatifs s'étendent aux fractions.

Théorème 4.5. *Le plus grand entier naturel inférieur à une fraction positive non réductible à un entier est le quotient du numérateur par le dénominateur. Cette fraction est la somme de ce quotient et d'une fraction ayant pour numérateur le reste de la division et pour dénominateur celui de la fraction donnée.*

Exemple 38.

$$\frac{21}{8} = 2 + \frac{5}{8} \qquad 2 < \frac{21}{8} < 3$$
$$\frac{3}{7} = 0 + \frac{3}{7} \qquad 0 < \frac{3}{7} < 1$$

Chapitre 5

Les polynômes

On suppose connues le notions élémentaires de polynôme vues depuis le lycée. Nous revoyons (sous forme d'activité) les opérations élémentaires sur les polynômes dans la section suivante : addition, multiplication et division.

5.1 Opérations

5.1.1 Addition

Considérons deux polynômes, par exemple

$$A(x) = 2x^6 + x^4 - x^3 - 5x + 1$$
$$B(x) = -x^3 + x^2 + x - 2$$

Ajoutons-les :

$$\begin{aligned} A(x) + B(x) &= (2x^6 + x^4 - x^3 - 5x + 1) + (-x^3 + x^2 + x - 2) \\ &= 2x^6 + x^4 - x^3 - 5x + 1 - x^3 + x^2 + x - 2 \\ &= 2x^6 + x^4 - 2x^3 + x^2 - 4x - 1 \end{aligned}$$

Démarche utilisée :

i) L'addition étant *associative*, nous avons pu supprimer les parenthèses.

ii) Puisqu'elle est *commutative*, nous avons mis côte à côte les monômes contenant les mêmes puissances de x.

iii) Enfin puisque la multiplication est *distributive* par rapport à l'addition, nous avons mis les diverses puissances de x en facteur.

Ces règles de calcul sont très élémentaires et très connues. Il est donc inutile de détailler avec autant de soin le pourquoi de ce calcul. Le plus important est de *pouvoir aller plus vite, en diminuant les risques d'erreurs*. Voici comment procéder.

On écrit les polynômes l'un en dessous de l'autre, puissance de x sous puissance correspondante de x, en ayant soin de laisser des blancs pour bien montrer que les puissances correspondantes sont manquantes.

$$\begin{array}{rcccccc} A(x) = & 2x^6 & +x^4 & -x^3 & & -5x & +1 \\ B(x) = & & & -x^3 & +x^2 & +x & -2 \\ \hline A(x)+B(x) = & 2x^6 & +x^4 & -2x^3 & +x^2 & -4x & -1 \end{array}$$

Il ne reste plus qu'à additionner, colonne par colonne, les coefficients des puissances de x.

Remarque. Dans l'exemple précédent, le *degré* de $A(x)+B(x)$ est 6, c'est celui de A.

Exemple 39. Donner un exemple de deux polynômes de degré 3 tels que la somme soit de degré 2.

5.1.2 Multiplication

Cherchons maintenant à multiplier les deux polynômes précédents en allant le plus vite possible, sans faire de fautes. Comment par exemple, trouver le coefficients de x^4 ? pour trouver des monômes en x^4 dans le produit, on peut

soit multiplier x^4 par -2 et obtenir $-2x^4$
soit multiplier $-x^3$ par x et obtenir $-x^4$
soit multiplier $-5x$ par $-x^3$ et obtenir $+5x^4$

Il vient donc au total $(-2-1+5)x^4 = 2x^4$
Mais il n'y a qu'une manière d'obtenir un monôme de degré 9 :

multiplier $2x^6$ par $-x^3$ et obtenir $-2x^9$.

Procédant ainsi pour tous les monômes par ordre de degrés décroissants de 9 à 0, on écrit

$$\begin{aligned} A(x)B(x) &= -2x^9+2x^8+(2-4)x^7+(-4+1+1)x^6+(1-1)x^5 \\ &\quad +(-2-1+5)x^4+(2-5-1)x^3+(-5+1)x^2+(10+1)x-2 \\ &= -2x^9+2x^8-2x^7-2x^6+2x^4-4x^3-4x^2+11x-2. \end{aligned}$$

On peut, à la fois pour gagner du temps, et rendre le texte plus lisible, faire des calculs de coefficients sur une feuille de brouillon auxiliaire, et écrire directement le résultat après le signe =. Avec un peu d'entraînement, il est même souvent inutile d'utiliser une feuille auxiliaire, un calcul mental évitant cet intermédiaire.

Remarque. Le degré du produit $A(x)B(x)$ est égal à 9 : c'est la somme des degrés des polynômes A et B.

Exos 2. On pose

$$\begin{aligned} A(x) &= 3x^2+2x-1 \\ B(x) &= x^3-x^2+x+2 \\ C(x) &= 2x^3-4x+5 \end{aligned}$$

Calculer les polynômes $A(x)^2, B(x)^2, C(x)^2, A(x)B(x)+B(x)C(x)+C(x)A(x), A(x)B(x)C(x)$, en ayant soin d'exposer les calculs le plus clairement et le plus proprement possible.

5.1.3 Division

Expliquons le mécanisme de cette nouvelle opération sur l'exemple suivant. Posons

$$\begin{aligned} A(x) &= 4x^5-6x^4+4x+1 \\ B(x) &= -x^4+x-1 \end{aligned}$$

et remarquons que le degré de A est supérieur à celui de B. On cherche un monôme $Q_1(x)$ tel que le polynôme

$$A_1(x) = A(x) - Q_1(x)B(x)$$

soit de degré inférieur à celui de $A(x)$, i.e ici 5. Il est facile de voir qu'il suffit pour cela de choisir

$$Q_1(x) = 4x^5 / -x^4 = -4x$$

i.e le quotient des monômes de plus haut degré des polynômes $A(x)$ et $B(x)$.
En effet, il vient avec cette valeur de $Q_1(x)$:

$$\begin{array}{rcccccc} A(x) & = & 4x^5 & -6x^4 & & +4x & +1 \\ \hline Q_1(x)B(x) & = & 4x^5 & & -4x^2 & +4x & \\ \hline A_1(x) & = & & -6x^4 & +4x^2 & & +1 \end{array}$$

Puisque le degré de $A_1(x)$ est supérieur à celui de $B(x)$, on peut recommencer l'opération. On pose donc

$$Q_2(x) = -6x^4 / -x^4 = 6 \qquad \text{et} \qquad A_2(x) = A_1(x) - Q_2(x)B(x)$$

$$\begin{array}{rcccccc} A_1(x) & = & -6x^4 & +4x^2 & & +1 & \\ \hline Q_2(x)B(x) & = & -6x^4 & & +6x & -6 & \\ \hline A_2(x) & = & & 4x^2 & -6x & +7 & \end{array}$$

Maintenant le degré de $A_2(x)$ est inférieur à celui de B, on ne peut plus recommencer. On dit que $A_2(x)$ est le reste de la division du polynôme A par le polynôme B. On pose

$$Q(x) = q_1(x) + Q_2(x) = -4x + 6$$

On dit que $Q(x)$ est le quotient de la division de A par B. Dans la pratique, on dispose l'opération de la façon suivante :

$$\begin{array}{cccccc|ccc} 4x^5 & -6x^4 & & +4x & +1 & & -x^4 & +x & -1 \\ \hline 4x^5 & & -4x^2 & +4x & & & -4x & +6 & \\ \hline & -6x^4 & +4x^2 & & +1 & & & & \\ & -6x^4 & & +6x & -6 & & & & \\ \hline & & 4x^2 & -6x & +7 & & & & \end{array}$$

Divisons de même le polynôme $A(x) = x^5 + x^4 + x^3 + x^2 + x + 1$ par $B(x) = x^3 + 2x + 3$. On obtient comme reste $-4x^2 + 4$ et comme quotient $x^2 + x - 1$.

Exos 3. On note $R(x)$ le reste et $Q(x)$ le quotient de la division de $A(x)$ par $B(x)$. Vérifier dans les deux exemples précédents que l'on a bien l'égalité

$$A(x) = B(x)Q(x) + R(x).$$

5.2 L'anneau des polynômes

5.2.1 Définitions

On se donne des nombres $a_0, a_1, \ldots, a_n$ et on considère la fonction $x \mapsto a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Cette fonction est usuellement appelée un polynôme ; les a_i, où i parcourt l'ensemble des valeurs 0, 1, ..., n sont ses coefficients ; si a_n est non nul, n est le degré du polynôme ; enfin x est la variable.

Considérons maintenant deux polynômes

$$A(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$
$$B(x) = b_3x^3 + b_2x^2 + b_1x + b_0.$$

Le coefficient de x^2 dans $A(x)+B(x)$ est a_2+b_2 ; mais celui de x^4 est a_4, et non a_4+b_4 puisque b_4 n'existe pas. De même le terme constant, les les coefficients de x, x^2, x^3 dans le produit $A(x)B(x)$ sont

$$\begin{array}{l} a_0b_0 \\ a_0b_1 \quad + \quad a_1b_0 \\ a_0b_2 \quad + \quad a_1b_1 \quad + \quad a_2b_0 \\ a_0b_3 \quad + \quad a_1b_2 \quad + \quad a_2b_1 \quad + \quad a_3b_0 \end{array}$$

Alors que le coefficient de x_4 est

$$a_1b_3 \quad + \quad a_2b_2 \quad + \quad a_3b_1 \quad + \quad a_4b_0$$

Pour avoir une formule analogue aux précédentes, devrait figurer dans cette expression un terme a_0b_4, qui ne peut évidemment pas y être.
Quand au coefficient de x^6 dans le produit $A(x)B(x)$

$$a_3b_3 + a_4b_2$$

il est encore plus "irrégulier", puisque par analogie avec les formules précédentes, on aurait aimé l'écrire

$$a_0b_6 \; + \; a_1b_5 \; + \; a_2b_4 \; + \; a_3b_3 \; + \; a_4b_2 \; + \; a_5b_1 \; + \; a_6b_0$$

ce qui n'a aucun sens ici car ni b_6, ni b_5, ni b_4, ni a_5, ni a_6 ne sont définis. Comment contourner la difficulté en écrivant des formules générales pour la somme et le produit sans être obligé de distinguer d'innombrables cas particuliers ? C'est facile !
On convient que b_4, b_5, ..., a_5, a_6, ... bref que *tous les coefficients qui ne figurent pas explicitement dans la donnée des polynômes $A(x)$ et $B(x)$ sont nuls.* Avec cette convention, le coefficient de x dans la somme $A(x)+B(x)$ est a_4+b_4 puisque l'on a bien $a_4+b_4=a_4$. Celui de x^6 dans le produit $A(x)B(x)$ est :

$$a_0b_6 \; + \; a_1b_5 \; + \; a_2b_4 \; + \; a_3b_3 \; + \; a_4b_2 \; + \; a_5b_1 \; + \; a_6b_0$$

qui est bien égal à $a_3b_3+a_4b_2$.

Comment trouver le coefficient de x^r dans le produit $A(x)B(x)$?
Par analogie avec ce qui précède, on voit qu'il faut procéder de la manière suivante : *on additionne tous les termes de la forme a_ub_v* où les entiers positifs ou nuls u et v vérifient l'égalité $u+v=r$; par exemple a_0b_r, a_1b_{r-1}, a_rb_0 sont de tels termes : il y en a en tout $r+1$. Le résultat de ce calcul se désigne par au choix l'une des expressions :

$$\sum_{u+v=r} a_ub_v, \qquad \text{ou} \qquad \sum_{u=0}^{r} a_ub_{r-u}, \qquad \text{ou} \qquad a_0b_r + a_1b_{r-1} + \cdots + a_rb_0.$$

Avant de donner une définition abstraite, considérons les polynômes à coefficients dans $\mathbb{Z}/n\mathbb{Z}$ par exemple $\mathbb{Z}/3\mathbb{Z}$. Soit $p(x) = \bar{1}x^3 - \bar{1}x$. N'oublions pas que $p(x)$ est la valeur de la fonction p pour la valeur de x de la variable. Ici, x ne peut prendre que les trois valeurs 0, 1 et 2, et le calcul est vite fait :

$$p(\bar{0}) = \bar{0}-\bar{0}=\bar{0} \quad p(\bar{1}) = \bar{1}-\bar{1}=\bar{0} \quad p(\bar{2}) = \bar{2}-\bar{2}=\bar{0}$$

Autrement dit, la fonction $x \mapsto p(x)$ est nulle, et pourtant l'être algébrique n'a pas l'air d'être nul. Nous allons maintenant donner une définition abstraite des polynômes en se basant sur la pratique acquise grâce aux calculs précédents.

Définition abstraite des polynômes

Nous désignerons par **K** un corps commutatif. Vous pourrez penser à $\mathbb{R}$, $\mathbb{Q}$ ou $\mathbb{C}$, mais aussi à $\mathbb{Z}/3\mathbb{Z}$ ou à d'autres corps de ce type. Tant que n'interviennent pas de divisions dans **K**, vous pouvez prendre $\mathbf{K} = \mathbb{Z}$.

Définition 10. On appelle *suite à valeurs dans* **K** *toute fonction* $u : \mathbb{N} \to \mathbf{K}$. *La valeur de la fonction u en* $n \in \mathbb{N}$ *est notée en générale* u_n. *On écrit souvent*

$$u = (u_n)_{n\in\mathbb{N}}$$

Définition 11. On appelle polynôme à coefficients dans **K** toute suite à valeurs dans **K**, $P = (P_n)_{n\in\mathbb{N}}$, possédant la propriété suivante :

$$\boxed{\text{il existe } n_0 \in \mathbb{N} \text{ tel que } n > n_0 \text{ implique } P_n = 0}$$

Autrement dit seulement un nombre fini des P_n est non nul. On dit aussi que les P_n sont nuls à partir d'un certain rang (ici $n_0 + 1$).
Les P_n sont appelés les *coefficients* de P, P_n étant le n^{e} coefficient.
On dit que deux polynômes P et Q sont *égaux* s'ils ont mêmes coefficients i.e $P_n = Q_n$ quel que soit $n = 0, 1, 2, ...$

Exemples

LE POLYNÔME NUL**.** C'est celui défini par les égalités $P_n = 0$ quel que soit n. On le désigne par 0.

LE POLYNÔME CONSTANT**.** Plus généralement soit $k \in \mathbf{K}$, on pose $P_0 = k$, $P_n = 0$ si $n > 0$. Le polynôme ainsi défini est appelé polynôme constant k et désigné par k.

LE POLYNÔME X. C'est celui dont tous les coefficients sont nuls sauf le premier qui vaut 1 : $X_n = 0$ pour $n \neq 1$, $X_1 = 1$.

LE POLYNÔME X^p. C'est celui dont tous les coefficients sont nuls sauf le p^{e} qui vaut 1 : $X^p_n = 0$ pour $n \neq p$, $X^p_p = 1$.
Remarquons que l'on a donc $X^1 = X$, $X^0 = 1$.

Degré d'un polynôme

On appelle degré du polynôme P et on note $\deg P$ le plus grand entier n tel que l'on ait $P_n \neq 0$. Puisque les P_n sont nuls pour n assez grand, un tel entier existe toujours sauf si les P_n sont tous nuls, donc sauf si $P = 0$.
On convient de poser $\deg 0 = -\infty$.
Si $\deg P = n > -\infty$, on dit que P_n est le coefficient dominant de P : c'est le coefficient du terme de plus haut degré de P. Il résulte des définitions que l'on a :

$$\deg 0 = -\infty, \quad \deg k = 0 \text{ si } k \neq 0, \quad \deg X = 1, \quad \deg X^p = p.$$

5.2.2 Arithmétique de $\mathbf{K}[X]$

On désigne par $\mathbf{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbf{K}$. Le X qui figure dans cette notation est destiné à nous rappeler que l'on a ainsi désigné le polynôme dont tous les coefficients sont nuls sauf le premier qui vaut 1.

Donnons-nous deux polynômes P et Q de $\mathbf{K}[X]$. On définit deux suites à valeurs dans $\mathbf{K}$, notées $P+Q$ et PQ par les égalités

$$(P+Q)_n = P_n + Q_n$$
$$(PQ)_n = \sum_{u+v=n} P_u Q_v$$

Proposition 5.1. *Les suites $P+Q$ et PQ sont des polynômes.*

Démonstration. Puisque P et Q sont des polynômes, il existe des entiers n_0 et n_1 tels que l'on ait $P_n = 0$ pour $n > n_0$ et $Q_n = 0$ pour $n > n_1$. Pour $n > \max\{n_0, n_1\}$ on a à la fois $P_n = 0$ et $Q_n = 0$. Ainsi, pour ces n, on a $(P+Q)_n = P_n + Q_n = 0$, et donc $P+Q$ est bien un polynôme. Choisissons maintenant $n > n_0 + n_1$ et considérons deux entiers u et v vérifiant $u+v=n$. Deux cas sont possibles : ou bien $u > n_0$ ou bien $u \leqslant n_0$; dans le premier cas, il vient $P_u = 0$ donc $P_u Q_v = 0$ et dans le second cas, il vient

$$v = n - u \geqslant n - n_0 > n_1$$

et par conséquent $Q_v = 0$ donc $P_u Q_v = 0$. Nous avons démontré :

$$\text{si } u+v = n > n_0 + n_1 \qquad \text{alors on a} \qquad P_u Q_v = 0.$$

Mais alors, par définition même du symbole $\sum_{u+v=n}$, il vient

$$(PQ)_n = \sum_{u+v=n} P_u Q_v = 0$$

pour $n > n_0 + n_1$, autrement dit, PQ est un polynôme. □

Exemples

- Pour tout P, on a $P+0 = 0+P = P \qquad P\cdot 0 = 0\cdot P = 0 \qquad P\cdot 1 = 1\cdot P = P$
- $X \cdot X = X^2$
- Plus généralement, quels que soient p et $q \geqslant 0$ on a

  $$X^p X^q = X^{p+q} = X^q X^p.$$

  En effet, pour qu'un terme $X_u^p X_v^q$ soit non nul, il faut et il suffit que l'on ait à la fois $u = p$ et $v = q$. Donc on a $(X^p X^q)_n = 0$ si $n \neq p+q$, et $(X^p X^q)_{p+q} = X_p^p X_q^q = 1$. Il vient donc $X^p X^q = X^{p+q}$. Échangeons p et q : on a $X^q X^p = X^{q+p} = X^{p+q}$ puisque $p+q = q+p$ dans $\mathbb{N}$.

Exos 4. Vérifiez que l'on a, quels que soient les entiers $p, q, r \leqslant 0$

$$(X^p X^q) X^r = X^p (X^q X^r)$$

⌟

A des polynômes P et Q nous avons associé de nouveaux polynômes, leur somme $P+Q$ et leur produit PQ. Nous allons comparer les degrés de ces nouveaux polynômes à ceux des polynômes donnés. Pour le faire en toute généralité, il nous faut au préalable introduire la convention suivante.
CONVENTION On pose

$$-\infty+(-\infty)=-\infty; \qquad -\infty<n; \qquad -\infty+n=n-\infty \quad \forall\, n\geqslant 0.$$

Théorème 5.2. *Soient P et Q des polynômes, on a*

$$\deg(P+Q)\leqslant \sup(\deg P,\ \deg Q)$$

(L'inégalité ne pouvant être stricte que si $\deg P=\deg Q$*)*

$$\deg PQ=\deg P+\deg Q.$$

Démonstration. Si $Q=0$, □

Remarque. Il est clair que $\deg(P+Q)=\deg P+\deg Q$ lorsque les degrés de P et Q sont différents. Mais lorsque P et Q ont même degré, celui de $P+Q$ peut diminuer par exemple si les coefficients dominants de P et Q sont opposés.

L'anneau des polynômes $\mathbf{K}[X]$

Nous venons de construire deux applications de $\mathbf{K}[X]\times\mathbf{K}[X]\to\mathbf{K}[X]$ appelés respectivement *somme* ou *addition* et *produit* ou *multiplication* et notées respectivement $+$ et $\cdot$. Ces opérations vérifient les règles de calcul suivantes :

a) – l'addition est **associative** et **commutative**
   – elle possède un **élément neutre**, le polynôme 0 : $0+P=P+0=P$
   – tout élément possède un **opposé** ; l'opposé de P noté $-P$, est le polynôme dont les coefficients sont donnés par les égalités : $(-P)_n=-P_n$; il est clair que l'on a $(-P)+P=P+(-P)=0$

b) – la multiplication est **associative** et **commutative**
   – elle possède un **élément neutre**, c'est le polynôme 1 : $1\cdot P=P\cdot 1=P$
   – elle possède un **élément nul (absorbant)**, c'est le polynôme 0 : $0\cdot P=P\cdot 0=0$

c) la multiplication est **distributive** par rapport à l'addition, i.e. que l'on a quels que soient les polynômes P, Q et R, l'égalité

$$(P+Q)\cdot R=P\cdot R+Q\cdot R.$$

Vous savez que l'on décrit la propriété a) en disant que l'opération $+$ munit $\mathbf{K}[X]$ d'une *structure de groupe commutatif* et l'ensemble des propriétés a), b) et c) en disant que $+$ et $\cdot$ munissent $\mathbf{K}[X]$ d'une *structure d'anneau commutatif*. On désignera donc $\mathbf{K}[X]$ sous le nom d'anneau des polynômes à coefficients dans $\mathbf{K}$.

Démonstration des propriétés a),b) et c). □

La multiplication par un scalaire : l'espace vectoriel $\mathbf{K}[X]$

Définissons une nouvelle opération $\mathbf{K} \times \mathbf{K}[X] \to \mathbf{K}[X]$ appelée *multiplication par les scalaires*. On pose, pour

$$k \in \mathbf{K} \quad \text{et} \quad P \in \mathbf{K}[X], \qquad (kP)_n = kP_n.$$

Ainsi, kP est le polynôme dont les coefficients sont obtenus, à partir de ceux de P, par multiplication de k.
On vérifie aisément sur les définitions les égalités

$$\deg(kP) = \begin{cases} \deg P & \text{si} \quad k \neq 0 \\ -\infty & \text{si} \quad k = 0 \end{cases}$$

ainsi que les propriétés
d) **associativité :**

$$k(k'P) = (kk')P \qquad \forall\, k, k' \in \mathbf{K}, \quad \forall\, P \in \mathbf{K}[X]$$

élément neutre : $1P = P1 = P$ où 1 est l'élément neutre de $\mathbf{K}$
distributivités :

$$(k+k')P = kP + k'P$$
$$k(P+P') = kP + kP'$$

quels que soient les scalaires k, k' de $\mathbf{K}$ et les polynômes P et P' de $\mathbf{K}[X]$.

On exprime les propriétés a) et d) en disant que $\mathbf{K}[X]$ est muni structure d'espace vectoriel sur le corps $\mathbf{K}$.

Remarque. Multiplions le polynôme constant k par P. On trouve le polynôme kP que l'on vient de définir (à vérifier !). Heureusement ! car sinon la notation kP aurait été ambigüe, désignant à la fois la multiplication de deux polynômes ou d'un scalaire par un polynôme. En particulier, les propriétés désignées par d) ne sont que des cas particuliers de propriétés b) ou c) lorsque certains polynômes sont constants.

5.2.3 La représentation usuelle des polynômes

On a déjà vu que $X^2 = X \cdot X$, $X^3 = X \cdot X \cdot X$; comme on a $X^p X^q = X^{p+q}$, on peut facilement noter que X^n est le produit de n facteurs égaux à X, c'est pourquoi le polynôme se lit «X puissance n».

Considérons maintenant des scalaires $\lambda_0, \lambda_1, \ldots, \lambda_r$, i.e des éléments de $\mathbf{K}$, et posons (on rappelle que l'on a $X^0 = 1$ et $X^1 = X$)

$$P = \lambda_0 X^0 + \lambda_1 X^1 + \cdots + \lambda_r X^r$$

(En théorie des espaces vectoriels, ceci est une combinaison linéaire de $X^0, \ldots, X^r$)

Lemme 5.3. *On a $P_n = \lambda_n$ si $n \leqslant r$ et $P_n = 0$ si $n > r$.*

Démonstration. Par définition de $+$ on a □

Théorème 5.4. *Tout polynôme s'écrit de manière unique comme combinaison linéaire des polynômes 1, X, X^2, ..., X^n, ... (on dit que l'ensemble $\{1, X, X^2, \ldots, X^n, \ldots\}$ est une base de $\mathbf{K}[X]$.)*

Démonstration. Soit P un polynôme, choisissons $r \geqslant \deg P$ □

Cas particulier important

On a

$$\boxed{a_0 + a_1X + \cdots + a_rX^r = 0 \quad \text{si et seulement si on a} \quad a_0 = a_1 = \cdots = a_r = 0}$$

Démonstration. Prenons $b_0 = b_1 = \cdots = b_r = 0$. Mais alors nous avons l'égalité $b_0 + b_1X + \cdots + b_rX^r = 0$. Mais par hypothèse, nous avons aussi

$$a_0 + a_1X + \cdots + a_rX^r = b_0 + b_1X + \cdots + b_rX^r.$$

D'après le théorème, nous pouvons écrire $a_0 = b_0$, $a_1 = b_1$, ..., $a_r = b_r$. □

5.3 Division euclidienne des polynômes

Nous allons dans cette section faire la théorie de l'opération appelée division euclidienne.

Théorème 5.5. *Le produit de deux polynômes est nul si et seulement si l'un des deux est nul.*

Démonstration. □

Corollaire 5.6 (Règle de simplification)**.** *si on a $AC = BC$ et $C \neq 0$, alors on a $A = B$.*

Théorème 5.7. *Soient A et B deux polynômes de $\mathbf{K}[X]$, B étant non nul. Il existe un et un seul polynôme Q tel que l'on ait l'inégalité*

$$\deg(A - BQ) < \deg B.$$

Théorie de la divisibilité

Cette théorie vous a été présentée pour l'anneau $\mathbb{Z}$ des entiers. Le théorème 5.7 qui permet de diviser des polynômes, permet ipso facto d'étendre la théorie à $\mathbf{K}[X]$. Les démonstrations seront formellement les mêmes, à la différence près que "les inégalités entre les entiers seront remplacées par les inégalités entre degrés des polynômes".

Définition 12. Soient A et B deux polynômes. On dit que B divise A et on écrit $B|A$, s'il existe un polynôme Q tel que l'on ait $A = BQ$. On dit encore que A est un multiple de B ou que B est un diviseur de A. Si B est non nul, il revient au même de dire que le reste de la division de A par B est nul (car $-\infty = \deg(A - BQ) < \deg B$ et l'inégalité est stricte puisque l'on a $B \neq 0$.)

Lemme 5.8. *Soient A, B et P des polynômes tels que l'on ait $P|A$ et $P|B$. Alors quels que soient les polynômes U et V, on a $P|AU + BV$.*

Lemme 5.9. *Soient A, B et P des polynômes tels que l'on ait $P|B$ et $B|A$. Alors on a $P|A$.*

Démonstration. □

Définition 13. On dit qu'un polynôme P est un diviseur commun à A et B si l'on a à la fois $P|A$ et $P|B$.

Nous allons terminer cette section par l'étude des diviseurs communs à deux polynômes.
Remarquons que si k est un scalaire non nul, alors on peut écrire

$$A = (k^{-1}A)k$$

et donc, on a $k|A$ quels que soient $k \neq 0$, $k \in \mathbf{K}$ et $A \in \mathbf{K}[X]$. Autrement dit, les scalaires non nuls sont des diviseurs communs de A et B.

Définition 14. On dit que A et B sont premiers entre eux si leurs seuls diviseurs communs sont les scalaires non nuls.

Théorème 5.10 (Théorème principal)**.** *Soient A et B deux polynômes. Alors il existe un polynôme Δ ayant les deux propriétés suivantes :*

i) *quels que soient les polynômes U et V, on a $\Delta \,|\, AU + BV$.*

ii) *il existe des polynômes U_0 et V_0 tels que l'on ait $\Delta = AU_0 + BV_0$.*

Si Δ' est un polynôme vérifiant les conditions i) *et* ii)*, il existe un scalaire $k \neq 0$ tel que l'on ait $\Delta' = k\Delta$.*

Énoncé équivalent : Soient A et B deux polynômes, et soit J l'ensemble des polynômes qui peuvent s'écrire $AU + BV$ lorsque U et V parcourent $\mathbf{K}[X]$. Cet ensemble J est formé de tous les multiples d'un polynôme Δ appartenant à J. Ce polynôme Δ est unique à la multiplication près par un scalaire non nul.

Démonstration. □

Remarque. Nous avons démontré au passage le résultat suivant :
«Les seuls polynômes inversibles [1] sont les constantes non nulles.»

Définition 15. On dit que Δ est le plus grand commun diviseur de A et B, en abrégé pgcd

Notation : On note $A \wedge B = \Delta$ (à un facteur non nul constant près).

Théorème 5.11 (Théorème de Bézout)**.** *Les polynômes A et B sont premiers entre eux si et seulement si il existe des polynômes U et V tels que l'on ait*

$$AU + BV = 1$$

Démonstration. □

Remarque. Lorsque l'on a $A \wedge B = 1$, tout polynôme $P \in \mathbf{K}[X]$ peut s'écrire sous la forme $AU + BV = P$. En effet, l'ensemble J des polynômes qui peuvent s'écrire ainsi est égal à l'ensemble des multiples du pgcd de A et B. Comme tout polynôme est un multiple de 1, c'est que $\mathbf{K}[X] = J$.

Recherche pratique du pgcd Le recherche pratique du pgcd utilise la proposition suivante :

Proposition 5.12. *Soient A et B deux polynômes et supposons* $\deg A \geqslant \deg B \geqslant 0$*. Soit R le reste de la division de A par B. Alors le* pgcd *de A et B est égal au* pgcd *de B et R.*

Comme les degrés de B et R sont respectivement plus petits que ceux de A et B, nous avons ramené la recherche du pgcd de A et B à un problème plus simple. Rien n'empêche de réitérer le procédé : on appelle R' le reste de la division de B par R si $R \neq 0$ et on a $A \wedge B = R \wedge R'$ etc. d'où le nom de la méthode :
`recherche du pgcd par la méthode des divisions successives.`

Démonstration. Démarche presque identique au cas des entiers. □

1. i.e les polynômes Λ pour lesquels il existe Λ' vérifiant $\Lambda\Lambda' = 1$

5.4 Calculs de PGCD

Exemple 40. Trouvez le pgcd Δ des deux polynômes

$$A = x^5 - 3x^4 + 2x^3 + x^2 - 3x + 2$$
$$B = x^4 - 2x^3 + 2x^2 - 7x + 6$$

Trouvez ensuite les polynômes U et V tels que l'on ait $AU + BV = \Delta$.

Solution.

Exemple 41. Montrez que les deux polynômes

$$A = x^6 + 2x^5 + 2x^4 + 3x^3 + 3x^2 + 2x$$
$$B = x^4 + 2x^3 + x^2 + x + 1$$

sont premiers entre eux. Trouvez deux polynômes U et V tels que l'on ait $AU + BV = 1$.

Solution.

Chapitre 6

Fractions rationnelles - Décomposition en éléments simples

Dans ce chapitre nous travaillerons avec l'anneau $\mathbf{K}[X]$ construit dans le chapitre précédent. Nous nous limiterons exclusivement à $K = \mathbb{R}$ ou $\mathbb{C}$.
Commençons juste par rappeler la définition suivante :

Définition 16. On dit qu'un polynôme P non nul est irréductible si les seuls diviseurs de P sont les polynômes de degré 0 ou les polynômes de degré égal à celui de P.

Ces polynômes jouent dans l'anneau $\mathbf{K}[X]$ un rôle analogue aux nombres premiers dans l'anneau des entiers $\mathbb{Z}$.

6.1 Fraction rationnelle, pôles et éléments simples

Définition 17.

- On dit que $F(x) = \dfrac{P(x)}{Q(x)}, P, Q \in \mathbf{K}[X]$ est une `fraction rationnelle irréductible` si et seulement si P et Q sont sans facteur commun.
- On appelle `pôles` de la fraction irréductible les racines du polynôme $Q(x)$.

Définition 18. Soit $Q(x) = a(x-z_1)^{m_1}(x-z_2)^{m_2}\cdots(x-z_p)^{m_p}(x^2+b_1x+c_1)^{n_1}\cdots(x^2+b_qx+c_q)^{n_q}$ la décomposition irréductible de $Q(x)$.

- On appelle `éléments simples de première espèce` relatifs aux pôles z_i, les m_i fonctions rationnelles du type

$$\frac{A_1}{x-z_i}, \quad \frac{A_2}{(x-z_i)^2}, \quad \cdots, \quad \frac{A_{m_i}}{(x-z_i)^{m_i}} \quad \text{où les } A_k \text{ sont des constantes réelles.}$$

- On appelle `éléments simple de deuxième espèce` relatifs aux polynômes irréductibles $x^2+b_jx+c_j$, les n_j fonctions rationnelles du type

$$\frac{B_1x+C_1}{x^2+b_jx+c_j}, \frac{B_2x+C_2}{(x^2+b_jx+c_j)^2}, \cdots, \frac{B_{n_j}x+C_{n_j}}{(x^2+b_jx+c_j)^{n_j}} \text{ où les } B_k, C_k \text{ sont des ctes réelles.}$$

Exemple 42. Décrire les éléments simples de

$$F(x) = \frac{P(x)}{Q(x)} = \frac{x^3-21x-7}{(x+2)(x-1)^2(x^2+x+1)}$$

Solution.

⋆ Éléments simples de 1ère espèce :
- Le pôle $x = 1$ est de multiplicité 2 donc est associé à 2 éléments simples

$$\frac{A_1}{x-1}, \quad \frac{A_1}{(x-1)^2};$$

- Le pôle $x = -2$ de multiplicité 1 est associé à un élément simple $\frac{A_3}{x+2}$

⋆ Éléments simples de 2e espèce :
1 seul élément simple de 2e espèce relatif au facteur irréductible x^2+x+1 ($\Delta < 0$) :

$$\frac{B_1 x + C_1}{x^2+x+1}.$$

NB : Assurez-vous de la décomposition complète du dénominateur.

Théorème 6.1. *Soit $F(x) = \frac{P(x)}{Q(x)}$ une fonction rationnelle irréductible. Alors*
- *Si $P(x) = Q(x)S(x) + R(x)$, $\deg(R(x)) < \deg(Q(x))$, on a $F(x) = S(x) + \frac{R(x)}{Q(x)}$.*
- *$\frac{R(x)}{Q(x)}$ se décompose de manière unique comme somme de tous les éléments simples relatifs à Q.*

Exemple 43. Donner la structure de la décomposition en éléments simples de

$$F(x) = \frac{x^3 - 21x - 7}{(x+2)(x-1)^2(x^2+x+1)}.$$

Solution.

$$F(x) = \frac{A_1}{x-1} + \frac{A_2}{(x-1)^2} + \frac{A_3}{x+2} + \frac{B_1 x + C_1}{x^2+x+1}. \tag{6.1}$$

6.2 Calcul des coefficients d'une décomposition en éléments simples

6.2.1 Pour les coefficients des pôles simples (multiplicité 1)

Notons α_i, i de tels pôles. Pour chaque i, on multiplie l'équation (6.1) par $x - \alpha_i$ et on prend $x = \alpha_i$. Ainsi, dans le membre de droite, il ne reste que A_i, dont la valeur est donnée par le membre de gauche : soit

$$\frac{P(\alpha_i)}{Q_i(\alpha_i)} \quad \text{avec} \quad Q_i(x) = \frac{Q(x)}{x - \alpha_i} \quad \text{i.e } x - \alpha_i \text{ simplifié dans } Q(x)$$

Exemple 44. En appliquant ce qui qu'on vient de décrire au pôle -2 pour trouver A_3, on a : En multipliant (6.1) par $x+2$, on a

$$\frac{x^3 - 21x - 7}{(x-1)^2(x^2+x+1)} = (x+2)\left(\frac{A_1}{x-1} + \frac{A_2}{(x-1)^2}\right) + A_3 + (x+2)\frac{B_1 x + C_1}{x^2+x+1}$$

En posant $x = -2$, on a $\frac{-8 + 21 \cdot 2 - 7}{9 \cdot 3} = A_3 = 1$.

6.2.2 Pour les coefficients des pôles multiples

Pour connaître le coefficient A_{im_i} qui correspond à un pôle d'ordre m_i, on multiplie par $(x-\alpha_i)^{m_i}$, puis on prend $x=\alpha_i$: de manière analogue à ce qui précède, on trouve le coefficient recherché.

Exemple 45. On détermine donc A_2 en multipliant (6.1) par $(x-1)^2$ puis en posant $x=1$. On obtient $A_2=-3$.

6.2.3 Pour les coefficients $B_{jn_j}C_{jn_j}$ des facteurs quadratiques

On peut appliquer la même méthode, mais avec les racines complexes des facteurs $x^2+b_jx+c_j$.
Pour cela, on multiplie par le facteur $(x^2+b_jx+c_j)^{n_j}$ puis on prend x égal à une des racines complexes du facteur, pour trouver (avec la partie réelle et imaginaire) les coefficients B_j et C_j.

Exemple 46. Dans notre exemple, $x^2+x+1=\dfrac{x^3-1}{x-1}$,
les racines sont donc les deux racines 3e non triviales de l'unité : $j=\mathrm{e}^{i2\pi/3}$ et $\overline{j}\mathrm{e}^{-i2\pi/3}$.
En multipliant (6.1) par x^2+x+1 et en prenant $x=j$, on trouve

$$B_1 j+C_1=-\frac{2+7j}{1-j}.$$

Ce qui donne (partie réelle et imaginaire) les coefficients B_1 et C_1 après un petit calcul. Cependant, ici ce calcul est un peu lourd et comme la simplicité et l'élégance sont souvent recherchées dans notre discipline, nous allons plutôt utiliser une autre méthode dite des limites.

6.2.4 Méthode des limites

Cette méthode consiste à multiplier d'abord par la plus basse puissance qui intervient dans la décomposition en éléments simples, et de prendre la limite lorsque $x\to\infty$ (où il suffit de garder les puissances les plus élevées). Ainsi, on a dans le membre de droite la somme des coefficients qui correspondent à cette puissance, qui permet de déterminer un coefficient en fonction des autres.

Exemple 47. Dans notre exemple, on multiplie par x, la limite donne alors

$$\lim_{x\to+\infty} xF(x)=\lim_{\infty}\frac{x^4}{x^5}=0=A_1+A_3+B_1$$

et donc $B_1=-A_1-A_3=-3$.

6.2.5 Méthode des valeurs particulières

Une autre méthode consiste à simplement prendre des valeurs particulières pour x (différentes des pôles) et ainsi d'avoir un système d'équations qui permettra de déterminer les coefficients manquants.

Exemple 48. Dans notre exemple, prenons $x = 0$: on a $\frac{-7}{2} = -A_1 + A_2 + \frac{A_3}{2} + C_1$. Ainsi, on obtient $C_1 = 1$.

Remarque. En général, il faut créer un système d'autant d'équations (indépendantes) qu'il reste de coefficients à déterminer.