DOCUMENT 2

La division euclidienne

La division euclidienne joue un role central en arithmétique. Comme c'est l'un des tous premiers résultats que l'on démontre, il est important de savoir exactement ce qui est connu lorsqu'on l'aborde. Nous supposerons ici que l'on a donné les définitions de $\mathbb{N}$ et de $\mathbb{Z}$ et que l'on a établi, comme dans le document 1, ou admis :

- La structure d'anneau commutatif et unitaire de $\mathbb{Z}$. Dans $\mathbb{Z}$ il n'y a pas de diviseur de zéro ($ab = 0$ implique $a = 0$ ou $b = 0$).
- Les relations élémentaires entre l'ordre sur $\mathbb{Z}$, définie par $a \leq b$ si et seulement si il existe $c \in \mathbb{N}$ tel que $a + c = b$, et la multiplication et l'addition. En particulier $a \leq b$ et $c \geq 0$ impliquent $ac \leq bc$.
- Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Un corollaire de ce dernier résultat est :

Toute partie non vide et minorée de $\mathbb{Z}$, admet un plus petit élément.

Preuve. Soit $X \subset \mathbb{Z}$, non vide et minoré par a. Si $a \geq 0$ alors X est contenu dans $\mathbb{N}$ et son plus petit élément dans $\mathbb{N}$ est aussi son plus petit élément dans $\mathbb{Z}$. Supposons maintenant $a < 0$ et soit $X^* = \{n - a \mid n \in X\}$. Si $n \in X$, $a \leq n$ d'où $0 \leq n - a$ et donc $X^* \subset \mathbb{N}$. Soit b le plus petit élément de X^*. Il existe $c \in X$ tel que $b = c - a$ et pour tout $n \in X$, $b \leq n - a$ d'où $c = a + b \leq n$ et c est le plus petit élément de X.

On peut trouver une démonstration un peu différente de ce résultat dans le document 1.

1. La division euclidienne dans $\mathbb{N}$ et $\mathbb{Z}$

THÉORÈME 2.1. *(Division euclidienne dans $\mathbb{Z}$). Soit $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :*

$$a = bq + r, \qquad 0 \leq r <\mid b \mid .$$

Les entiers q et r sont appelés, respectivement, le quotient et le reste de la division euclidienne de a par b.

Preuve de l'existence.

Si $a = 0$ alors le couple $(0, 0)$ convient. Supposons $a \neq 0$.

1^{er} cas : $b > 0$. Soit $A = \{n \in \mathbb{Z} \mid nb > a\}$. L'entier $(\mid a \mid +1)b$ est un multiple de b qui est strictement plus grand que a. En effet :

$$(\mid a \mid +1)b >\mid a \mid b =\mid a \mid (b - 1 + 1) \geq \mid a \mid \geq a.$$

On a donc $A \neq \emptyset$. Montrons que A est minoré par $-|a|$:

si $m < -|a|$ alors, comme $b \geq 1$, $mb < -|a|b \leq -|a| \leq a$ et donc $m \notin A$.

Soit n le plus petit élément de A. De $n-1<n$ on déduit $(n-1)b<nb$ et donc $(n-1)b\leq a<nb$. Posons $q=n-1$. On a $qb\leq a<qb+b$ d'où $0\leq a-qb<b$. Si $r=a-qb$ alors $a=bq+r$ et $0\leq r<b=\mid b\mid$.

2^{me} cas : $b<0$. D'après le premier cas, il existe q et r tels que $a=(-b)q+r$ avec $0\leq r\leq\mid -b\mid$. En écrivant $a=b(-q)+r$, on voit que le couple $(-q,r)$ convient.

Preuve de l'unicité.

Supposons que :

$$a=bq+r,\ 0\leq r<\mid b\mid$$

$$a=bq'+r',\ 0\leq r'<\mid b\mid .$$

On a $r'-r=b(q-q')$. Or $-\mid b\mid<r'-r<\mid b\mid$, ou encore, $-\mid b\mid<b(q-q')<\mid b\mid$. Il en résulte que $0\leq\mid b\mid\mid q-q'\mid<\mid b\mid$ et donc $0\leq\mid q-q'\mid<1$. Finalement, $\mid q-q'\mid=0$ d'où $q=q'$ et $r=r'$.

THÉORÈME 2.2. *(Division euclidienne dans $\mathbb{N}$). Soit $a\in\mathbb{N}$, $b\in\mathbb{N}^*$. Il existe un unique couple $(q,r)\in\mathbb{N}^2$ tel que :*

$$a=bq+r,\qquad 0\leq r<b.$$

Preuve. L'unicité résulte de l'unicité dans $\mathbb{Z}$. Pour l'existence, considérons la preuve du théorème 1 dans le cas $b>0$. Comme $nb>a$, on a $n>0$ et donc $q=n-1\geq 0$. De plus, $r<\mid b\mid=b$ et donc $(q,r)\in\mathbb{N}^2$ et vérifie

$$a=bq+r,\qquad 0\leq r<b.$$

Remarques.

1) **La descente de Fermat.** Il existe une variante de la démonstration de l'existence du quotient et du reste dans le cas de deux entiers positifs a et b connue sous le nom de descente de Fermat. Supposons $0<b\leq a$ (sinon $(0,a)$ convient). Il existe q_1 tel que $q_1b\leq a$. Soit $r_1=a-bq_1$. Si $r_1<b$ alors (q_1,r_1) convient et sinon $r_1\geq b$ et il existe q_2 tel que $q_2b\leq r_1$. Soit $r_2=r_1-bq_2$. Si $r_2<b$ le couple (q_1+q_2,r_2) convient et sinon $r_2\geq b$ et on continue. Comme $r_1>r_2>\ldots$, on ne peut pas toujours avoir $r_n\geq b$ et il existe un plus petit entier k pour lequel $r_k<b$ et $(q_1+q_2+\cdots+q_k,r_k)$ est le couple cherché.

2) La preuve donnée ici de l'existence du couple (q,r) est constructive en ce sens qu'il est facile d'en déduire un programme permettant de calculer effectivement ce couple. Il existe des preuves beaucoup plus courtes mais qui n'ont pas cette qualité. Par exemple, dans le cas de deux entiers a et b positifs on peut faire une démonstration par récurrence sur a. On a $0=0.b+0$ et si $a=bq+r$ avec $0\leq r<b$ alors $a+1=bq+(r+1)$. Si $r+1<b$ alors $(q,r+1)$ convient et si $r+1=b$ alors $a+1=(q+1)b$.

3) L'entier bq n'est pas toujours le multiple de b le plus proche de a (Exemple : $19=3.5+4.$). On peut montrer que pour tout $(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$ il existe $(q',r')\in\mathbb{Z}^2$ tel que $a=bq'+r'$ avec $|r'|\leq\dfrac{|b|}{2}$. L'entier bq' est alors un multiple de b rendant $|a-bq'|$ minimum. Si $a=bq+r$, $0\leq r<|b|$ alors $(r',q')=(r,q)$ si $0\leq r\leq\dfrac{|b|}{2}$ et $(r',q')=(r-b,q+1)$ sinon.

Exercice Si $x \div y$ désigne le quotient de la division euclidienne de x par y alors montrer que, pour trois entiers strictement positifs a, b et c,

$$a \div (bc) = (a \div b) \div c.$$

Solution. Posons $a = bq + r$, $0 \leq r < b$, et $q = cq' + r'$, $0 \leq r' < c$. On a $a = b[cq' + r'] + r = bcq' + br' + r$ et de $0 \leq r' \leq c - 1$ on déduit $0 \leq br' \leq bc - b$ d'où $br' + r \leq bc - b + r < bc$ car $r - b < 0$. Finalement $q' = a \div c$.

On peut utiliser le résultat précédent en calcul mental. Par exemple : $311 \div 21 = (311 \div 3) \div 7 = 103 \div 7 = 14$.

2. Applications

La division euclidienne étant au tout début de l'arithmétique, ses applications font intervenir en général des notions qui apparaissent à un stade plus avancé de cette discipline.

2.1. Détermination des sous-groupes de $\mathbb{Z}$. Il est clair que pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe de $\mathbb{Z}$ ($na+nb = n(a+b)$, $-(na) = n(-a)$). Réciproquement, soit G un sous-groupe de $\mathbb{Z}$. Si $G = \{0\}$ alors $G = 0\mathbb{Z}$ et si $G \neq \{0\}$ alors G possède un élément non nul m. On a aussi $-m \in G$ et donc $G^+ = \{n \in \mathbb{Z} \mid n \in G,\, n > 0\} \neq \emptyset$. Soit n_0 le plus petit élément de G^+. Le groupe G contient tous les multiples de n_0 et si $n \in G$ alors il existe $(q, r) \in \mathbb{Z}^2$ tel que

$$n = n_0 q + r,\ 0 \leq r < n_0$$

On a $r = n - n_0 q \in G$ et donc, par définition de n_0, $r = 0$ d'où $n = n_0 q$ et finalement $G = n_0\mathbb{Z}$. Supposons que $G = m\mathbb{Z}$ avec $m \in \mathbb{Z}$. On a $m \in n_0\mathbb{Z}$ d'où l'existence de $a \in \mathbb{Z}$ tel que $m = n_0 a$. De même, il existe $b \in \mathbb{Z}$ tel que $n_o = mb$ et $m = abm$ d'où $ab = 1$. On a donc $a = b = 1$ ou $a = b = -1$. Dans le premier cas on a $m = n_0$ et dans le second, $m = -n_0$. On a démontré :

Proposition 2.1. *Tous les sous-groupes de $\mathbb{Z}$ sont monogènes (c'est-à-dire engendrés par un seul élément). Tout sous-groupe, distinct de $\{0\}$, possède un unique générateur strictement positif et un unique générateur strictement négatif. Ces générateurs sont opposés l'un de l'autre.*

Remarques

1) Tous les sous-groupes de $\mathbb{Z}$, distincts de $\{0\}$, sont isomorphes à $\mathbb{Z}$ et donc isomorphes entre eux. Un isomorphisme de $\mathbb{Z}$ sur $n\mathbb{Z}$ est l'application $m \in \mathbb{Z} \to nm \in n\mathbb{Z}$. En revanche, deux quotients distints $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$ ne sont jamais isomorphes.

2) Les ensembles de la forme $n\mathbb{Z}$, $n \in \mathbb{Z}$, sont aussi les sous-anneaux et les idéaux de l'anneau $\mathbb{Z}$. Un anneau est dit principal s'il est intègre (commutatif,unitaire, non réduit à $\{0\}$ et sans diviseur de 0) et si tous ses idéaux sont principaux. L'anneau $\mathbb{Z}$ est un exemple d'anneau principal.

3) Détermination de l'ensemble des idéaux de l'anneau des nombres décimaux. Voir le document 7.

2.2. Les groupes cycliques. Un groupe G est dit cyclique s'il est fini et engendré par un élément (G est formée par les puissances positives et négatives d'un élément).

Soit a un générateur d'un groupe cyclique G. Le groupe G étant fini, l'application $n \in \mathbb{N}^* \to a^n$ n'est pas injective et il existe des entiers strictement positifs p et q tels que $p < q$ et $a^p = a^q$. Si e désigne l'élément neutre de G alors $e = a^{q-p}$. Il existe donc des entiers strictement positifs l tels que $a^l = e$. Soit d le plus petit et

$$X = \{a^0 = e, a, a^2, \ldots, a^{d-1}\}.$$

Tous les élément de X sont distincts car si $a^p = a^q$ avec $0 \leq p \leq q \leq d-1$ alors $a^{q-p} = e$ avec $0 \leq q-p < d$ et donc $q-p = 0$. Soit $a^k \in G$ avec $k \in \mathbb{Z}$. Il existe $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $k = qd + r$ et $0 \leq r \leq d-1$. On a $a^k = (a^d)^q a^r = a^r$ d'où $a^k \in X$ et finalement $G = X$. On a donc montré que si G est un groupe cyclique ayant d éléments alors

$$G = \{a^0 = e, a, a^2, \ldots, a^{d-1}\}.$$

On peut montrer que tous les groupes cycliques d'ordre d sont isomorphes et en particulier isomorphes à $\mathbb{Z}/d\mathbb{Z}$.

Maintenant, soit G un groupe fini d'ordre n et a un élément de G. Le sous groupe engendé par a est cyclique et s'il est d'ordre d alors, par le théorème de Lagrange, d divise n. On a donc $a^d = e$ avec d un diviseur de n.

2.3. Numération. En général, un système de numération est formé par une suite finie de symboles, appelés chiffres, et d'un algorithme associant de façon injective à chaque entier une suite finie de ces symboles. Cette suite est appelée l'écriture de l'entier (dans le système de numération donné). Par exemple dans la numération romaine, les chiffres sont I, V, X, C, M, ... , à l'entier neuf on associe IX, à l'entier douze est associé XII. En principe, un bon système de numération permet de déterminer par un algorithme simple l'écriture de la somme ou du produit de deux entiers à l'aide des écritures de chacun de ces entiers. Il doit aussi être facile de comparer deux entiers en utilisant uniquement leurs écritures.

Nous allons d'abord démontrer le résultat mathématique qui est le fondement du système de numération en base b, $b \geq 2$, et plus particulièrement du système décimal.

PROPOSITION 2.2. *Soit $(a,b) \in \mathbb{N}^2$ avec $b \geq 2$ et $((q_n, r_n))_n$ la suite de $\mathbb{N}^2$ définie par récurrence de la façon suivante :*

- *(q_0, r_0) est formé par le quotient et le reste de la division euclidienne de a par b ;*
- *(q_{n+1}, r_{n+1}) est formé par le quotient et le reste de la division euclidienne de q_n par b.*

a) Il existe un plus petit entier n_0 tel que $k \geq n_0$ entraine $q_k = r_{k+1} = 0$.
b) On a : $a = r_{n_0} b^{n_0} + \ldots + r_2 b^2 + r_1 b + r_0$.
c) Si $a = s_p b^p + \ldots + s_2 b^2 + s_1 b + s_0$ avec $0 \leq s_i < b$ alors, pour tout entier k, $r_k = s_k$.

Preuve.

Remarque préliminaire. Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^*$. Il existe $(q,r) \in \mathbb{N}^2$ tel que $a = bq + r$ et $0 \leq r < b$. Si $b \geq 2$ alors on a $a \geq bq = (b-1)q + q \geq q$ et $a = q$ entraine $(b-1)q = 0$ d'où $q = 0 = a$ et aussi $r = 0$.

a) La remarque préliminaire implique que la suite (q_n) est décroissante. Elle est donc stationnaire à partir d'un certain rang car l'ensemble de ses termes possède un plus petit élément. Soit n_0 le plus petit entier tel que $q_{n_0} = q_{n_0+1}$. La remarque entraine $q_{n_0} = q_{n_0+1} = 0$ et, comme (q_n) décroit, $q_n = 0$ si $n \geq n_0$. On a aussi $r_n = 0$ si $n \geq n_0 + 1$ et $r_{n_0} \neq 0$.

Disons que n_0 est le rang de a. Une remarque, essentielle pour la suite de la preuve, est que la suite de $\mathbb{N}^2$ associée à l'entier q_0 est $((q_{n+1}, r_{n+1}))$ et si $n_0 \neq 0$ alors le rang de q_0 est $n_0 - 1$. On peut aussi remarquer que les entiers de rang 0 sont ceux compris entre 0 et $b-1$.

b) La démonstration se fait par récurrence sur le rang n_0 de a. Si $n_0 = 0$ alors $a = r_0 = r_{n_0}$ et le résultat est vrai. Supposons le résultat vrai pour tout entier de rang $n_0 - 1$ et soit a de rang n_0. L'entier q_0 étant de rang $n_0 - 1$ on a

$$q_0 = r_{n_0} b^{n_0-1} + r_{n_0-1} b^{n_0-2} + \ldots + r_2 b + r_1$$

et $a = bq_0 + r_0$ entraine

$$a = r_{n_0} b^{n_0} + ... + r_1 b + r_0$$

Le résultat est vrai pour n_0.

c) La démonstration se fait par récurrence sur le rang n_0 de a. Si $n_0 = 0$ alors $0 \leq a \leq b-1$ d'où $s_p = s_{p-1} = ... = s_1 = 0$ (car sinon $a \geq s_p b_p + ... + s_1 b \geq b$) et $s_0 = r_0$. Ainsi, on a bien $s_n = r_n$ pour tout entier n. Supposons maintenant c) pour tout entier de rang $n_0 - 1$ et soit a de rang n_0. On a :

$$a = bq_0 + r_0 = (s_p b^{p-1} + ... + s_1)b + s_0$$

avec $0 \leq s_0 \leq b-1$. L'unicité du quotient et du reste dans une division euclidienne entraine $q_0 = s_p b^{p-1} + ... + s_1$ et $s_0 = r_0$. Par l'hypothèse de récurrence on a $s_k = r_k$ si $k \geq 1$ et le résultat est vrai pour l'entier n_0.

La numération en base b et la numération décimale. Dans le système de numération en base b, $b \geq 2$, on représente les b premiers entiers par des symboles appelés chiffres. Désignons par $\overline{x}$ le chiffre associé à l'entier $x < b$. La proposition précédente, partie b), montre que tout entier positif a est déterminé par b et une suite finie r_0, r_1, ..., $r_{n_0} \neq 0$ d'entiers strictement inférieurs à b. L'écriture de a en base b est formée par les $n_0 + 1$ chiffres $\overline{r_{n_0}}\ \overline{r_{n_0-1}}....\overline{r_0}$. Par exemple en base dix (numération décimale), les chiffres sont 0, 1, 2, ...,9 et l'écriture de l'entier seize est 16 car $\overline{r_0} = 6$, $\overline{r_1} = 1$ et $r_n = 0$ si $n \geq 2$.

L'écriture d'un entier négatif n est obtenue en faisant précéder l'écriture de $-n$ du signe $-$.

Ecriture décimale des nombres rationnels. Soit $a = \dfrac{p}{q}$, $p \in \mathbb{N}$, $q \in \mathbb{N}^*$, un nombre rationnel positif. On définit par récurrence deux suites d'entiers (a_n) et (r_n) :

- a_0 et r_0 sont le quotient et le reste de la division euclidienne de p par q : $p = a_0 q + r_0$, $0 \leq r_0 < q$. On remarque que a_0 est la partie entière de $a = \dfrac{p}{q}$.
- Pour $n \geq 1$, a_n et r_n sont le quotient et le reste de la division euclidienne de $10 r_{n-1}$ par q : $10 r_{n-1} = a_n q + r_n$ et $0 \leq r_n < q$.

On montre que $0 \leq a_n < 10$ si $n \geq 1$ et que la suite (a_n) est périodique à partir d'un certain rang car il n'y a que q valeurs possibles pour r_n. Plus particulièrement, cette suite est nulle à partir d'un certain rang si et seulement si $a = \dfrac{p}{q}$ est un nombre décimal. Pour obtenir l'écriture en base 10 de a, lorsque ce nombre n'est pas un entier, on écrit de gauche à droite :

- l'écriture en base 10 de a_0
- une virgule
- les chiffres $\overline{a_1}\ \overline{a_2}\ ....\overline{a_n}\ ...$ (Cette suite est infinie mais, comme elle est périodique à partir d'un certain rang, on peut la caractériser sans trop d'ambiguité en écrivant qu'un nombre fini de ces premiers termes et des pointillés)

L'ecriture d'un nombre rationnel négatif r est obtenue en faisant précéder l'écriture de $-r$ du signe $-$.

2.4. Les congruences. Soit $n \geq 1$ un entier. Deux entiers p et q sont congrus modulo n si et seulement si ils ont même reste dans leurs divisions euclidiennes par n (voir le document 5). La division euclidienne est donc utile dans l'étude des congruences mais son rôle ne semble pas essentiel. Il est cependant intéressant de remarquer la grande similitude de signification des deux énoncés suivants :

(1) Pour tout entier $n \geq 1$, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ldots, \overline{r}, \ldots, \overline{n-1}\}$;

(2) Pour tout entier $p \geq 1$, il existe un unique entier $r \in [0, n-1]$ et un entier q (nécessairement unique) tel que $p = qn + r$.

2.5. Développement en fractions continues des nombres rationnels. Voir le document du fascicule 2 "Suites adjacentes,....".

2.6. L'algorithme d'Euclide. Voir le document 3.1.

Cet algorithme, qui permet de déterminer de façon pratique le PGCD de deux entiers p et q, a lui-même de nombreuses applications. Par exemple la détermination d'un couple de coefficients de Bezout pour ces entiers ou la décomposition en fraction continue du nombre rationnel $\frac{p}{q}$.

3. Compléments : les anneaux euclidiens.

Il existe aussi une division euclidienne dans les anneaux de polynômes $K[X]$. Pour obtenir une généralisation commune à $\mathbb{Z}$ et $K[X]$ on introduit la notion d'anneau euclidien.

Par définition, un anneau intègre A est dit euclidien s'il existe une application ϕ de $A^* = A \setminus \{0\}$ dans $\mathbb{N}$ telle que

1) Si $x \in A^*$, $y \in A^*$ et $y = xz$ avec $z \in A$ alors $\phi(x) \leq \phi(y)$.

2) Pour tout $(a, b) \in A \times A^*$, il existe $(q, r) \in A^2$ tel que

$$a = bq + r,\ r = 0 \text{ ou } r \neq 0 \text{ et } \phi(r) < \phi(b).$$

L'unicité du couple (q, r) n'est pas exigée et parfois le premier axiome de la définition est omis.

Les anneaux $\mathbb{Z}$ et $K[X]$ sont euclidiens. Dans $\mathbb{Z}$, il suffit de considérer $\phi(x) =\mid x \mid$ et dans $K[X]$, $\phi(P) = deg(P)$. On verra dans le document 7 que l'anneau $\mathbb{D}$ des nombres décimaux est euclidien et c'est la division euclidienne dans $\mathbb{Z}$ qui permet de l'établir.

Les anneaux euclidiens sont principaux et, comme dans tout anneau principal, on peut généraliser les notions de PGCD et de PPCM et démontrer l'existence d'une décomposition en facteurs premiers appelés ici facteurs irréductibles.

Un autre exemple d'anneau euclidien est donné par les entiers de Gauss $\mathbb{Z} + i\mathbb{Z} = \{a + ib | (a, b) \in \mathbb{Z}^2\}$. Ici on a $\phi(a + ib) = a^2 + b^2$.