Fiche 101 Niveau : 1 version 2 (1/05/2010) **Jaune**

Arithmétique de base - PGCD -PPCM

1 Introduction

L'arithmétique est l'étude de $\mathbb{Z}$ (et de $\mathbb{N}$) ainsi que de la division euclidienne dans $\mathbb{Z}$ (ou dans $\mathbb{N}$). Il existe plusieurs façons d'aborder et de concevoir les résultats de ce domaine des mathématiques. L'une est plutôt constructive et montre l'existence de certains objets (par exemple le pgcd ou le ppcm) en les construisant effectivement par un algorithme déterministe, l'autre consiste à montrer l'existence des mêmes objets par des considérations théoriques. Du point de vue de la rigueur, il n'y a pas de différence notable. En revanche sur le plan des résultats la différence est grande. Dans le premier cas, on est capable de mener à bien un certain nombre de calculs effectifs, dans le deuxième cas on acquiert une plus grande vision conceptuelle de la situation, ce qui amène souvent à des développements ultérieurs fructueux. De ce fait on aurait tort d'opposer ces deux points de vue, qui au contraire méritent d'être développés simultanément. Ces divers éclairages de l'objet d'étude en fournissent sans nul doute une compréhension beaucoup plus profonde. Dans cette fiche nous essairons de laisser une place à ces deux aspects.

Revenons à la division euclidienne dans $\mathbb{Z}$ qui est l'opération de base de l'arithmétique. Si a et b sont deux entiers et si b est différent de 0, il existe un couple unique (q, r) d'entiers tels que les deux conditions suivantes soient réalisées :

$$a = qb + r$$

$$0 \leq r < b.$$

L'entier q est appelé le **quotient** dans la division euclidienne de a par b, et r est appelé le **reste** de cette même division.

Toujours dans l'hypothèse où $b \neq 0$, on dit que a **est divisible** par b si le reste de la division euclidienne de a par b est nul, c'est-à-dire s'il existe un nombre q (nécessairement unique) tel que $a = qb$.
Si a est b sont dans $\mathbb{Z}$ on dira que a est multiple de b s'il existe q tel que $a = qb$. On note $b\mathbb{Z}$ l'ensemble de tous les multiples de b. Si b est non nul alors il est équivalent de dire a multiple de b ou b divise a et le nombre q tel que $a = qb$ est unique. Si $b = 0$, alors $a = 0$ est le seul multiple de b et quel que soit $q \in \mathbb{Z}$ on a $a = qb = 0$. On peut alors énoncer l'équivalence suivante, qui semble une trivialité, mais sur laquelle va reposer un grand nombre de développements ultérieurs :

$$a \text{ multiple de } b \text{ si et seulement si } a\mathbb{Z} \subset b\mathbb{Z}.$$

Par cette vision des choses on voit qu'on ramène l'étude de la relation de divisibilité à l'étude d'une inclusion entre certains sous-ensembles : des sous-ensembles de multiples. Pour préciser un petit peu plus on peut constater que la divisibilité dans $\mathbb{Z}$ est une **relation de préordre** (sur $\mathbb{N}$ c'est une relation d'ordre) et que cette relation correspond à la relation d'inclusion entre les sous-ensembles de multiples.
Une partie de l'arithmétique repose sur l'étude de cette relation de divisibilité et donc comme on vient de le voir sur le comportement des sous-ensembles de multiples. Par ailleurs, s'agissant d'une

relation d'ordre sur $\mathbb{N}$, il sera utile d'introduire la borne inférieure de deux éléments (**le plus grand commun diviseur** quand l'un des deux nombres est non nul) ainsi que leur borne supérieure (**le plus petit commun multiple**).

2 Sous-ensembles de multiples

Les sous-ensembles de multiples vérifient un certain nombre de propriétés algébriques. Plus précisément :

Théorème 2.1 *Soit $A = a\mathbb{Z}$ le sous-ensemble des multiples de a dans $\mathbb{Z}$, alors :*

1. *A est un sous-groupe additif de $\mathbb{Z}$,*
2. *pour tout x dans $\mathbb{Z}$ et tout y dans A, le produit xy est dans A.*

Preuve. Pour montrer que A est un sous-groupe du groupe additif $\mathbb{Z}$, il suffit de constater que si x et y sont des multiples de a, il en est de même de $x-y$. Pour la deuxième propriété on voit immédiatement que si y est un multile de a, alors pour tout x dans $\mathbb{Z}$, xy est aussi un multiple de a. □

Théorème 2.2 *Réciproquement si A est un sous-ensemble de $\mathbb{Z}$ vérifiant les deux propriétés*

1. *A est un sous-groupe additif de $\mathbb{Z}$,*
2. *pour tout x dans $\mathbb{Z}$ et tout y dans A, le produit xy est dans A,*

alors A est un sous-ensemble de multiples, c'est-à-dire est de la forme $a\mathbb{Z}$.

Preuve. Si A est réduit à $\{0\}$, il est bien de la forme indiquée, c'est le sous-ensemble constitué des multiples de 0. Sinon, il existe dans A un plus petit élément strictement positif qu'on notera a. Pour tout $x \in A$, par division euclidienne on peut écrire :

$$x = qa + r \quad \text{où } 0 \leq r < a.$$

Comme $r = x - aq$, on peut dire que $r \in A$. Et comme a est le plus petit élément strictement positif de A on peut dire que $r = 0$. Autrement dit x est multiple de a. □

Définition 2.3 *Un sous-ensemble de $\mathbb{Z}$ vérifiant les deux propriétés du théorème précédent est appelé un idéal. Ainsi les sous-ensembles de multiples sont les idéaux de $\mathbb{Z}$.*

Théorème 2.4 *Les idéaux de $\mathbb{Z}$ sont aussi les noyaux des homomorphismes de $\mathbb{Z}$ dans un anneau.*

Preuve. Soit f un homomorphisme de $\mathbb{Z}$ dans un anneau B. Il est immédiat de voir que si x et y sont dans $\ker(f)$ alors $f(x-y) = f(x) - f(y) = 0$, ce qui prouve que $\ker(f)$ est un sous-groupe de $\mathbb{Z}$. D'autre part si $y \in \ker(f)$, pour tout $x \in \mathbb{Z}$ on a $f(xy) = f(x)f(y) = 0$. Donc $\ker(f)$ est un idéal de $\mathbb{Z}$. Si maintenant A est un idéal de Z définissons dans $\mathbb{Z}$ la relation

$$x \mathcal{R} y \text{ si et seulement si } x - y \in A.$$

Cette relation est une relation d'équivalence. □

Il existe un certain dombre d'opérations intéressantes sur les idéaux, en particulier l'intersection et la somme. L'intersection de deux idéaux est l'intersection au sens ensembliste. La somme de deux idéaux est définie par :

$$I_1 + I_2 = \{y \in \mathbb{Z} \mid y = x_1 + x_2 \text{ où } x_1 \in I_1, x_2 \in I_2\}.$$

Théorème 2.5 *Soient I_1 et I_2 deux idéaux de $\mathbb{Z}$, alors $I_1 \cap I_2$ et $I_1 + I_2$ sont des idéaux de $\mathbb{Z}$.*

Preuve. On vérifie immédiatement en revenant aux définitions que si y et z sont dans $I_1 \cap I_2$ (resp. $I_1 + I_2$) alors il en est de même de $y - z$. Donc $I_1 \cap I_2$ (resp. $I_1 + I_2$) est un sous-groupe de $\mathbb{Z}$. On vérifie aussi que si y est dans $I_1 \cap I_2$ (resp. $I_1 + I_2$) et a dans $\mathbb{Z}$ alors ay est dans $I_1 \cap I_2$ (resp. $I_1 + I_2$). □

3 Le pgcd et le ppcm

Théorème 3.1 *Soient a et b deux entiers dont l'un au moins est non nul. Il existe un plus grand entier > 0 qui soit diviseur commun de a et de b. Cet entier noté pgcd(a, b) est appelé le plus grand commun diviseur de a et b. De plus, tout diviseur commun de a et de b divise pgcd(a, b).*

Preuve. Nous donnerons au paragraphe suivant un algorithme produisant le pgcd de deux éléments (et le ppcm), ce qui en prouvera l'existence. Cependant nous donnons ici une preuve théorique liée à l'interprétation de la divisibilité en terme d'inclusions d'idéaux, ainsi que nous l'avons remarqué précédemment.
Si un nombre c divise a et b alors on a les deux inclusions :

$$a\mathbb{Z} \subset c\mathbb{Z},$$

$$b\mathbb{Z} \subset c\mathbb{Z}.$$

En conséquence, on a aussi

$$a\mathbb{Z} + b\mathbb{Z} \subset c\mathbb{Z}.$$

Mais $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$ non réduit à $\{0\}$ puisque l'un au moins des entiers a et b est non nul. Il existe donc un unique $d > 0$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On a alors les propriétés suivantes :

$$a\mathbb{Z} \subset d\mathbb{Z},$$

$$b\mathbb{Z} \subset d\mathbb{Z},$$

pour tout diviseur c de a et b :

$$d\mathbb{Z} \subset c\mathbb{Z}.$$

Les propriétés que nous venons de mettre en évidence montrent que $d > 0$ divise a et b, et que tout diviseur de a est b divise d. En conséquence d est le plus grand diviseur de a et b. □

Lorsque le plus grand commun diviseur de a et b est 1, on dit que a et b sont **premiers entre eux**. Si on écrit $a = k_1 d$ et $b = k_2 d$ où $d = \text{pgcd}(a, b)$ alors k_1 et k_2 sont premiers entre eux (sinon on pourrait construire un diviseur commun de a et de b strictement plus grand que d).

Théorème 3.2 *Soient a et b deux entiers. Il existe un plus petit entier ≥ 0 qui soit multiple de a et de b. Cet entier noté ppcm(a, b) est appelé le plus petit commun multiple de a et b. De plus tout multiple commun de a et de b est multiple de ppcm(a, b).*

Preuve. On fait une démonstration analogue à celle du théorème précédent en utilisant cette fois-ci l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$. Le ppcm est le nombre $m \geq 0$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. □

En conclusion, on peut écrire :

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \text{ où } d = \text{pgcd}(a, b),$$

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \text{ où } m = \text{ppcm}(a, b).$$

En particulier on obtient le théorème de Bezout (que nous étudierons plus en détail dans une autre fiche)

Théorème 3.3 *Si a et b sont deux entiers dont l'un au moins est non nul, et si $d =$ pgcd(a, b) alors il existe des entiers u et v tels que $ua + vb = d$.*
Si a et b sont deux entiers tels qu'il existe u et v vérifiant $ua + vb = 1$ alors a et b sont premiers entre eux.

Preuve. La première partie découle de l'égalité $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Si maintenant il existe u et v tels que $ua + vb = 1$ il est clair que tout diviseur commun de a et b divise 1. □

Le théorème d'Euclide-Gauss en découle :

Théorème 3.4 *Si c divise un produit ab et s'il est premier avec a alors il divise b.*

Preuve. Si c est premier avec a alors il existe u et v tels que $ua + vc = 1$. Donc $uab + vcb = b$. Or c divise uab et vcb, donc il divise b. □

Revenons maintenant au pgcd et au ppcm. Nous pouvons établir une relation entre ces deux notions.

Théorème 3.5 *Soient a et b deux entiers dont l'un au moins est non nul. Alors :*

$$ppcm(a, b)pgcd(a, b) = |ab|.$$

Preuve. Si l'un des nombres a ou b est nul le résultat se voit immédiatement. Supposons donc $a > 0$ et $b > 0$. Soit $d =$ pgcd(a,b). Alors on écrit $a = k_1 d$ et $b = k_2 d$ où k_1 et k_2 sont premiers entre eux. Si z est un multiple commun de a et de b on a :

$$z = \alpha_1 k_1 d = \alpha_2 k_2 d,$$

donc :

$$\alpha_1 k_1 = \alpha_2 k_2.$$

Comme k_1 est premier avec k_2 on en conclut que k_1 divise α_2, et que par suite $z = \alpha_2 k_2 d = \alpha k_1 k_2 d$. Par conséquent tout multiple de a et de b s'écrit $\alpha k_1 k_2 d$. Mais $k_1 k_2 d$ est lui-même un multiple de a et de b, donc c'est le plus petit. On a finalement :

$$\text{ppcm}(a, b) = k_1 k_2 d = \frac{a}{d} \times \frac{b}{d} \times d = \frac{ab}{\text{pgcd}(a, b)}.$$

□

4 Algorithme de calcul du pgcd

4.1 Algorithme d'Euclide

$R0 := |a|$;
$R1 := |b|$; $\quad (b \neq 0)$
Tant que $R1 > 0$ **faire**
  $R := Reste\_Division(R0, R1)$;
  $R0 := R1$;
  $R1 := R$;
fintq ;

En sortie $R1 = 0$, et $R0 = \text{pgcd}(a, b)$.

Les conditions :

$$\begin{cases} \text{L'ensemble des diviseurs communs de } R0 \text{ et } R1 \text{ est} \\ \quad \text{l'ensemble des diviseurs communs de } a \text{ et } b. \\ \\ R_1 \geq 0 \end{cases}$$

constituent un invariant de boucle.
Remarquons qu'initialement l'ensemble des diviseurs communs de $R0$ et $R1$ est l'ensemble des diviseurs communs de a et de b. Notons $R0', R1'$ les nouvelles valeurs de $R0, R1$ en sortie d'un tour de boucle. Nous avons alors $R0' = R1$ et $R1' = R0 - QR1$ avec $0 \leq R1' < R1$. Donc tout diviseur de $R1$ et $R0$ est diviseur de $R0'$ et $R1'$, et réciproquement.
Cet algorithme se termine car $R1$ décroît strictement à chaque tour de boucle. A la fin $R1 = 0$, donc l'ensemble des diviseurs de $R0$ et de $R1$ est l'ensemble des diviseurs de $R0$, et par conséquent $R0 = \text{pgcd}(a, b)$.
Remarquons qu'on a prouvé au passage :

Théorème 4.1 *Les diviseurs communs de a et b sont les diviseurs de pgcd(a, b).*

relation qu'on avait déjà prouvée précédemment par l'étude des idéaux.