Chapitre 1

pgcd et ppcm

[...] **Rappel** Propriétés de réduction du pgcd :

- $\text{pgcd}(a;b) = \text{pgcd}(a-kb;b)$ pour tout $k \in \mathbb{N}$
- Si $0 < b \leq a$, $\text{pgcd}(a;b) = \text{pgcd}(b;r)$
- Si $b > 0$ divise a, $\text{pgcd}(a;b) = b$

Exemple Soit $n \in \mathbb{N}$, $a = 7n+4$ et $b = 5n+3$. Prouvons que a et b sont premiers entre eux.

$$\begin{aligned}
\text{pgcd}(a;b) &= \text{pgcd}(7n+4;5n+3) \\
&= \text{pgcd}(7n+4-5n-3;5n+3) = \text{pgcd}(2n+1;5n+3) \\
&= \text{pgcd}(2n+1;5n+3-2(2n+1)) = \text{pgcd}(2n+1;n+1) \\
&= \text{pgcd}(2n+1-2(n+1);n+1) = \text{pgcd}(-1;n+1) \\
&= 1
\end{aligned}$$

On peut aussi éliminer n :

$$5a - 7b = -1$$

Tout diviseur de a et de b doit nécessairement diviser -1, donc le pgcd de a et b est 1
Voir aussi Exercice corrigé 1p71
→ **Exercice** 4,6p87
Cherchons le pgcd de 600 et 375 en utilisant $\text{pgcd}(a;b) = \text{pgcd}(b;r)$ pour $0 < b \leq a$:

$600 = 1 \times 375 + 225$ donc $\text{pgcd}(600;375) = \text{pgcd}(375;225)$
$375 = 1 \times 225 + 150$ donc $\text{pgcd}(175;225) = \text{pgcd}(225;150)$
$225 = 1 \times 150 + 75$ donc $\text{pgcd}(225;150) = \text{pgcd}(150;75)$
$150 = 2 \times 75 + 0$ donc $r = 0$ et $\text{pgcd}(150;75) = 75$

Le pgcd est le dernier reste non nul de cette cascade de divisions euclidiennes.
Voir aussi Exemple en haut de la page 72.

A Algorithme d'Euclide

Proposition | Algorithme d'Euclide
Soit a et b deux entiers positifs tels que $b < a$. L'algorithme suivant, appelé algorithme d'Euclide, permet de calculer en un nombre fini d'étapes $\text{pgcd}(a;b)$.

1. Calculer le reste r de la division euclienne de a par b
2. Si $r = 0$ alors $pgcd(a; b) = b$
3. Si $r \neq 0$ alors on remplace a par b et b par r et on retourne à l'étape 1

Preuve :

1. $a = bq_0 + r_0$ avec $0 < r_0 < b$
   - $r_0 = 0$: alors l'algorithme termine et rend bien $\text{pgcd}(a; b) = b$
   - $r_0 \neq 0$: alors $\text{pgcd}(a; b) = \text{pgcd}(b; r_0)$ et l'algorithme continue avec b et $r_0 (< b)$ à la place de a et b respectivement.
2. $b = r_0q_1 + r_1$ avec $0 < r_1 < r0$
   - $r_1 = 0$: alors l'algorithme termine et rend bien $\text{pgcd}(b; r_0) = r_0$
   - $r_1 \neq 0$: alors $\text{pgcd}(b; r_0) = \text{pgcd}(r_0; r_1)$ et l'algorithme continue avec r_0 et $r_1 (< r_0)$ à la place de b et r_0 respectivement.

   On voit que l'on construit une liste strictement décroissante d'entiers positifs :

$$b > r_0 > r_1 > r_2 > \cdots \geq 0$$

   Cette liste est nécessairement finie. Notons r_k le dernier reste non nul :

$$r_{k-2} = r_{k-1}q_k + r_k$$

$$\text{et } r_{k-1} = r_kq_{k+1}$$

   Donc $\text{pgcd}(a, b) = r_k$ □

Voir Programme sur calculatrice p73
→ **Exercices** 16,17,19,18 pages 87,88

Corollaire (diviseurs communs et pgcd)
Soit a et b deux entiers relatifs non tous les deux nuls. Tout diviseur commun de a et b est aussi diviseur de $\text{pgcd}(a; b)$. Autrement dit, $\text{pgcd}(a; b)$ est un multiple de tout diviseur de a et b.
Preuve : On peut supposer a et b positifs car deux nombres opposés ont les mêmes diviseurs. Supposons $0 \leq b \leq a$.
- Si $b = 0$, alors $\text{pgdc}(a; b) = a$ et le corollaire est clairement vrai.
- Si $b > 0$, alors
  - Si b divise a, $\text{pgcd}(a; b) = b$ et le corollaire est clairement vrai.
  - Sinon, prenons les notations de l'algorithme d'Euclide, et utilisons la propriété 1 :

$$D(a; b) = D(b; r_0) = D(r_0; r_1) = \cdots = D(r_{k-1}; r_k) = D(r_k; 0)$$

    Autrement dit, l'ensemble des diviseurs communs de a et b est l'ensemble des diviseurs de $r_k = \text{pgcd}(a; b)$ □

Proposition (homogénéité)
Soit a et b deux entiers relatifs. Soit k un entier relatif non nul. On a

$$\text{pgcd}(ka; kb) = k \times \text{pgcd}(a; b)$$

Preuve : Si a ou b est nul ou si a divise b (ou b divise a) c'est évident. Sinon, lorsque l'on utilise l'algorithme d'Euclide avec ka et kb, on trouve les mêmes égalités que pour a et b multipliées par k. Par exemple pour les dernières :

$$kr_{k-2} = kr_{k-1}q_k + kr_k$$

$$\text{et } kr_{k-1} = kr_k q_{k+1}$$

D'où le résultat.

Exemple pgcd$(48;120) = 24$pgcd$(2;5) = 24 \times 1 = 24$

Corollaire (Propriété caractéristique)
Soit a et b des entiers relatifs non tous les deux nuls. Soit $d \in \mathbb{N}^\star$.
$d =$pgcd$(a;b)$ si et seulement si il existe a' et b' premiers entre eux tels que $a = da'$ et $b = db'$
Preuve :
- Si $d =$pgcd$(a;b)$, alors d divise a et b. Il existe donc a' et b' tels que $a = da'$ et $b = db'$. Par la proposition précédente, pgcd$(a;b) = d\times$pgdc$(a';b')$. Donc pgcd$(a';b') = 1$.
- Réciproquement, si il existe a' et b' premiers entre eux tels que $a = da'$ et $b = db'$, On a $d = d \times 1 = d\times$pgdc$(a';b') =$pgcd$(da';db') =$pgcd$(a;b)$

Conséquence : pour simplifier la fraction $\frac{a}{b}$ et la rendre irréductible, il suffit de simplifier a et b par pgcd$(a;b)$

Proposition (Décomposition en facteurs premiers)
Soit $a, b \geq 2$ deux entiers. S'ils ne sont pas premiers entre eux, $d =$pgdc$(a;b)$ est égal au produit des facteurs premiers communs à a et b, chaque facteur étant affecté du plus petit exposant avec lequel il figure dans leurs deux décompositions.
Preuve : a et b n'étant pas premiers entre eux, on a $d > 1$. Regardons la décomposition en nombres premiers de a et b (α_i et β_i pouvant être nuls) :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$$

Tout diviseur commun de a et b est de la forme :

$$p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n}$$

avec $0 \leq \gamma_i \leq$min$(\alpha_i;\beta_i)$ Donc le plus grand commun diviseur s'obtient en prenant les plus grand γ_i possible, c'est à dire le plus petit exposant entre α_i et β_i.

Exemple On cherche le pgcd de 23400 et 5616. On a
- $23400 = 2^3 \times 3^2 \times 5^2 \times 13$
- $5616 = 2^4 \times 3^3 \times 13$

Donc pgcd$(a;b) = 2^3 \times 3^2 \times 13 = 936$
→ **Exercice** 1p87

B Théorème de Bézout

Théorème Soit u, v deux entiers. Soit $d =$pgcd$(u;v)$.

1. Il existe deux entiers relatifs a et b tels que

$$au + bv = d$$

2. L'ensemble des nombres de la forme $au + bv$ est l'ensemble des multiples de d

Preuve : Pour le premier point, on reprend les notations de l'algorithme d'Euclide. Pour trouver les nombres a et b il suffit d'exprimer les restes r_i en fonction de u et v. On commence par r_0, puis on continue avec r_1, r_2, ... jusqu'à r_k qui est le nombre d.
Pour le second point, il faut prouver que deux ensemble sont égaux. Pour cela il suffit de prouver que le premier est inclus dans le second et que le second est inclus dans le premier.

- $\subset$ Soit un nombre $au + bv$. Le nombre d est un diviseur de u et de v, donc d divise $au + bv$. Donc $au + bv$ est un multiple de d.
- $\supset$ Soit dn un multiple de d. On sait d'après le premier point qu'il existe a et b tels que $d = au + bv$. Alors $dn = (an)u + (bn)v$ est bien de la forme voulue. □

Exemple trouver l'égalité de Bézout avec l'exemple donné pour Euclide.