LEÇON N^{O} 6

PGCD et PPCM dans $\mathbb{Z}$. Applications.

Clément BOULONNE

Session 2020

Préambule

Niveau de la leçon

Collège, Terminale S Spé

Prérequis

Divisibilité dans $\mathbb{Z}$, division euclidienne, multiples, diviseurs, nombres premiers et décomposition d'un entier en produit de facteurs premiers.

Références

— T. MOUADDEB, *PGCD, PPCM de deux nombres entiers. Nombres premiers entre eux, Bézout.* Leçon de Math, S2, Master 1 Ens. Math, 2010-2011.
— Contributeurs de WIKIPÉDIA, *Algorithme d'Euclide*, Wikipédia.

Table des matières

1 PGCD (plus grand commun diviseur)

Définition 1.1 (Plus grand commun diviseur). Soient a, b deux nombres entiers relatifs non nuls. L'ensemble des diviseurs communs de a et de b admet un plus grand élément que l'on appelle le *plus grand commun diviseur* de a et de b.

Remarques 1.2.

1. $b \mid a$ si et seulement si $\mathrm{PGCD}(a, b) = b$.
2. Soient a et b deux entiers relatifs :

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(|a|, |b|).$$

PROPRIÉTÉS 1.3. Étant donnés quatre nombres entiers a, b, c et d.

1. $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, a)$;
2. $\mathrm{PGCD}(ka, kb) = k\,\mathrm{PGCD}(a, b)$ avec $k \in \mathbb{Z}$.
3. Si $a \mid c$ et $b \mid d$ alors $\mathrm{PGCD}(a, b) \mid \mathrm{PGCD}(c, d)$.

Démonstration des propriétés 1.3. $\Diamond$

1. Triviale
2. Soit $k \neq 0$, on peut appliquer l'algorithme d'Euclide sur a et b :

$$\begin{cases} a = bq_0 + r_0 \\ b = r_0 q_1 + r_1 \\ r_0 = r_1 q_2 + r_2 \\ \quad \vdots \\ r_{n-2} = r_{n-1} q_n + r_n \\ r_{n-1} = r_n q_{n+1} + 0 \end{cases} \tag{1}$$

   Donc, d'après (1), $\mathrm{PGCD}(a, b) = r_n$. On multiplie les expressions de (1) par k :

$$\begin{cases} ka = kbq_0 + kr_0 \\ kb = kr_0 q_1 + kr_1 \\ kr_0 = kr_1 q_2 + kr_2 \\ \quad \vdots \\ kr_{n-2} = kr_{n-1} q_n + kr_n \\ kr_{n-1} = kr_n q_{n+1} + 0 \end{cases}$$

   D'où $\mathrm{PGCD}(ka, kb) = kr_n$.
3. Comme $\mathrm{PGCD}(a, b) \mid a$, $a \mid c$ et $\mathrm{PGCD}(a, b) \mid b$ et $b \mid d$ alors $\mathrm{PGCD}(a, b)$ divise c et d donc divise $\mathrm{PGCD}(c, d)$.

□

THÉORÈME 1.4 (THÉORÈME D'EUCLIDE). Soient a et b deux entiers non nuls. La suite des diviseurs euclidiennes :

— de a par b : $a = bq_0 + r_0$;
— de b par r_0 (si $r_0 \neq 0$) : $b = q_1 r_0 + r_1$;
— ...
— de r_{n-1} par r_n (si $r_n \neq 0$) : $r_{n-1} = r_n q_{n+1} + r_{n+1}$

fini par s'arrêter un des restes r_i étant nul. Le dernier reste non nul est alors le $\mathrm{PGCD}(a,b)$ (si $r_0 = 0$ alors $\mathrm{PGCD}(a,b) = b$).

Démonstration du théorème 1.4. $\Diamond$ Les inégalités $b > r_0 > r_1 > \cdots > r_n > \cdots \geq 0$ montrent que la suite $(r_k)_{k\in\mathbb{N}}$ est une suite décroissante d'entiers naturels, cette suite est finie. D'autre part, considérons l'égalité $a = bq_0 + r_0$:

— tout diviseur de a et b divise $a - bq_0$, c'est un diviseur de b et r_0 ;

— tout diviseur de b et r_0 divise $bq_0 - r_0$, c'est un diviseur de b et r_0.

Ainsi, les diviseurs communs de a et b sont ceux de b et r_0 et il va de même pour le plus grand d'entre eux : $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,r_0)$.

On peut appliquer ce raisonnement à chaque égalité :

$$\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,r_0) = \cdots = \mathrm{PGCD}(r_{i-1},r_{i-2}).$$

Or si $r_{i-2} = r_{i-1}q_i + 0$ alors $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(r_{i-1},r_i) = r_{i-1}$ avec $r_i = 0$. □

On donne maintenant un algorithme qu'on peut écrire sur Xcas :

```
pgcdeuclide(a,b):={
   local r;
   tantque b<>0 faire
     r := irem(a,b)
     a := b
     b := r
  ftantque
   retourne(a)
}
```

Exemple 1.5. Calculer $\mathrm{PGCD}(1636, 1128)$.

Exemple 1.5. $\Diamond$ On applique l'algorithme d'Euclide :

$$\begin{aligned}
1636 &= 1128 + 508\\
1128 &= 2\times 508 + 112\\
508 &= 4\times 112 + 60\\
112 &= 60 + 52\\
60 &= 52 + 8\\
52 &= 6\times 8 + 4\\
8 &= 4\times 2 + 0.
\end{aligned}$$

Donc : $\mathrm{PGCD}(1636, 1128) = 4$. □

2 PPCM

Définition 2.1. Soient a et b deux entiers naturels non nuls. L'ensemble des multiples communs strictement positifs de a et b admet un plus petit élément appelé le ***PPCM*** de a et b, noté $\mathrm{PPCM}(a,b)$.

Remarques 2.2.

1. Les multiples communs à a et b sont les multiples du $\mathrm{PPCM}(a,b)$.
2. $a \mid n$ et $b \mid n$ si et seulement si $\mathrm{PPCM}(a,b) \mid n$.

Exemple 2.3. $\mathrm{PPCM}(6, 15) = 30$.

PROPRIÉTÉS 2.4.
1. $\mathrm{PPCM}(a,b) = \mathrm{PPCM}(b,a)$.
2. Soit $k \in \mathbb{Z}$, $\mathrm{PPCM}(ka,kb) = k\,\mathrm{PPCM}(a,b)$.
3. Si $a \mid c$ et $b \mid d$ alors $\mathrm{PPCM}(a,b) \mid \mathrm{PPCM}(c,d)$.

◊ *Démonstration de la proposition 2.4.*
1. Triviale par définition.
2. Soit $m = \mathrm{PPCM}(a,b)$. Il existe donc p et q entiers relatifs tels que $m = pa = qb$ donc $km = kap = kbp$ et donc km est un multiple commun à a et b. Ainsi $\mathrm{PPCM}(ka,kb) \leq k\,\mathrm{PPCM}(a,b)$.
   Soit $M = \mathrm{PPCM}(ka,kb)$. Il existe p' et q' entiers relatifs tels que $M = p'ka = q'kb$. donc a divise $\frac{M}{k}$ qui est entier car multiple commun de a et b, donc $\mathrm{PPCM}(a,b) \leq \frac{\mathrm{PPCM}(ka,kb)}{k}$. On en déduit que $\mathrm{PPCM}(ka,kb) = k\,\mathrm{PPCM}(a,b)$.
3. Comme $a \mid c$ alors $a \mid \mathrm{PPCM}(c,d)$ et $b \mid d$ donc $b \mid \mathrm{PPCM}(c,d)$. Ainsi, $\mathrm{PPCM}(a,b) \mid \mathrm{PPCM}(c,d)$.

□

3 PPCM et PGCD

3.1 Une proposition

PROPOSITION 3.1. Soient a et b deux entiers relatifs non nuls. On a :

$$\mathrm{PGCD}(a,b) \cdot \mathrm{PPCM}(a,b) = |ab|\,.$$

◊ *Démonstration de la proposition 3.1.* Soient $D = \mathrm{PGCD}(a,b)$ et $M = \mathrm{PPCM}(a,b)$. Il existe a' et b' tels que $a = Da'$ et $b = Db'$ avec $\mathrm{PGCD}(a',b') = 1$.

$$\begin{aligned} DM &= \mathrm{PGCD}(Da',Db') \times \mathrm{PPCM}(Da',Db') \\ &= D^2 \times \mathrm{PGCD}(a',b') \times \mathrm{PPCM}(a',b') \\ &= D^2 \times 1 \times \mathrm{PPCM}(a',b') \end{aligned}$$

On pose $m = \mathrm{PPCM}(a',b')$ et on a :

$$a'b' \geq m. \tag{2}$$

Comme $a' \mid m$, $b' \mid m$ et $\mathrm{PGCD}(a',b') = 1$, d'après Gauss, $a'b' \mid m$, d'où

$$a'b' \leq m. \tag{3}$$

De (2) et (3), on obtient $m = a'b'$ donc

$$Dm = D^2a'b' = Da'Db' = ab.$$

□

4 Applications

4.1 Nombres premiers entre eux

Définition 4.1. Soient a et b deux entiers relatifs non nuls, a et b sont *premiers entre eux* si et seulement si $\mathrm{PGCD}(a,b) = 1$.

PROPRIÉTÉ 4.2. Soient a et b deux entiers naturels non nuls. δ est le PGCD de a et de b si et seulement si, $\frac{a}{\delta}$ et $\frac{b}{\delta}$ sont des entiers premiers entre eux.

Démonstration de la propriété 4.2. $\Diamond$ On justifie que $\frac{a}{\delta}$ et $\frac{b}{\delta}$ sont des entiers naturels non nuls.

Comme $\delta = \text{PGCD}(a, b)$, $\delta \mid a$ et $\delta \mid b$ donc il existe deux entiers relatifs k et k' tels que $k\delta = a$ et $k'\delta = b$, d'où $\delta = \frac{a}{k} = \frac{b}{k'}$.

$$\frac{a}{\delta} = \frac{a}{\frac{a}{k}} = a \times \frac{k}{a} = k \in \mathbb{Z}$$
$$\frac{b}{\delta} = \frac{b}{\frac{b}{k'}} = b \times \frac{k'}{b} = k' \in \mathbb{Z}.$$

Si $d = \text{PGCD}(\frac{a}{\delta}, \frac{b}{\delta})$ alors, en utilisant la formule d'homogénéité, on obtient :

$$d = \text{PGCD}(\tfrac{a}{\delta}, \tfrac{b}{\delta}) = \frac{1}{\delta}\,\text{PGCD}(a, b).$$

Or $\delta = \text{PGCD}(a, b)$ d'où $d = 1$.

Réciproquement, si $\frac{a}{\delta}$ et $\frac{b}{\delta}$ sont premiers entre eux alors $\text{PGCD}(\frac{a}{\delta}, \frac{b}{\delta}) = 1$. En utilisant une nouvelle fois, la formule d'homogénéité :

$$\text{PGCD}(\tfrac{a}{\delta}, \tfrac{b}{\delta}) = \frac{1}{\text{PGCD}(a, b)}\,\text{PGCD}(a, b) = 1$$

et ainsi, $\delta = \text{PGCD}(a, b)$. □

Exemple 4.3. Factoriser $\frac{12345}{13991}$.

Exemple 4.3. $\Diamond$ On calcule $\text{PGCD}(12345, 13991)$.

$$13991 = 12345 \times 1 + 1646$$
$$12345 = 1646 \times 7 + 823$$
$$1646 = 823 \times 2 + 0.$$

Donc : $\text{PGCD}(12345, 13991) = 823$ et :

$$12345 = 15 \times 823$$
$$13991 = 17 \times 823$$

D'où :

$$\frac{12345}{13991} = \frac{15}{17}.$$

Comme $\text{PGCD}(15, 17) = 1$, la fraction $\frac{15}{17}$ est irréductible. □

THÉORÈME 4.4 (THÉORÈME DE GAUSS). Soient a, b et c trois entiers relatifs non nuls. Si $a \mid bc$ et a et$b$ sont premiers entre eux alors $a \mid c$.

Démonstration du théorème 4.4. $\Diamond$ Comme $a \mid bc$, il existe un entier k tel que $bc = ka$. Comme a et b sont premiers entre eux, d'après le théorème de Bézout, il existe des entiers relatifs u et b tels que $au + bv = 1$.

En multipliant par c cette dernière égalité, on obtient :

$$c = acu + bcv = acu + kav = a(cu + kv).$$

Comme $(cu + kv)$ est un entier, cette égalité prouve que $a \mid c$. □

PROPOSITION 4.5. Soient a, b et c trois entiers relatifs. Si $a \mid c$, $b \mid c$, a et b sont premiers entre eux alors $ab \mid c$.

Démonstration de la proposition 4.5. $\Diamond$ Comme $a \mid c$, il existe $d \in \mathbb{Z}$ tel que $c = ad$. Comme $b \mid c$, il existe $d' \in \mathbb{Z}$ tel que $c = bd'$. Donc $ad = bd'$. Comme a divise bd' et $\mathrm{PGCD}(a, b) = 1$, d'après le théorème de Gauss, a divise d'. Il existe donc $d'' \in \mathbb{Z}$ tel que $d' = ad''$. Donc :

$$c = d'b = ad''b.$$

□

4.2 Égalité de Bézout

THÉORÈME 4.6. Soient a et b deux entiers relatifs non nuls et d leur PGCD. Alors il existe des entiers relatifs u et v tels que $au + bv = d$. On appelle cette égalité, *égalité de Bézout*.

Démonstration du théorème 4.6. $\Diamond$

— Soit E l'ensemble des entiers naturels non nuls de la forme $ax + by$ où x et y sont des entiers relatifs.
E est une partie non vide de $\mathbb{N}$. En effet, on a, par exemple, $|a| \in E$ car, selon le signe de a, l'entier naturel $|a|$ s'écrit $a \times 1 + b \times 0$ ou $a \times (-1) + b \times 0$. E étant une partie non vide de $\mathbb{N}$, E admet un plus petit élément n.
Par définition de E, il existe donc des entiers relatifs u et v tels que $n = au + bv$. Or d divise a et b donc d divise n, d'où $d \leq n$.

— On montre que n divise a en écrivant la division euclidienne de a par n : $a = nq + r$ avec $0 \leq r < n$ et $q \in \mathbb{Z}$. Donc :

$$r = a - nq = a - q(au + bv) = a(1 - qu) + b(-qv).$$

Ainsi r est de la forme $ax + by$ avec x et y des entiers relatifs. De plus, $r < n$ donc, par définition de n, $r \notin E$. Alors nécessairement $r = 0$ et donc n divise a.

— On montre de même que n divise b. D'où, par définition de d, $n \leq d$. Finalement, on obtient $d = n = au + bv$.

□

THÉORÈME 4.7 (THÉORÈME DE BÉZOUT). Deux entiers relatifs a et b sont premiers entre eux si et seulement si il existe des entiers relatifs u et v tels que $au + bv = 1$.

Démonstration du théorème 4.7. Si a et b sont premiers entre eux alors $\mathrm{PGCD}(a, b) = 1$ et donc, avec la propriété précédente, $au + bv = 1$.

Réciproquement, on suppose qu'il existe des entiers relatifs u et v tels que $au + bv = 1$. Soit $D = \mathrm{PGCD}(a, b)$ alors D divise a, D divise b donc D divise $au + bv$, d'où $D = 1$. □

Exemple 4.8. Résoudre l'égalité de Bézout suivante :

$$266u + 224v = \mathrm{PGCD}(266, 224).$$

Exemple 4.8. $\Diamond$ On détermine tout d'abord $\mathrm{PGCD}(266, 244)$ avec l'algorithme d'Euclide :

$$\begin{aligned} 266 &= 1 \times 224 + 42 \\ 224 &= 5 \times 42 + 14 \\ 42 &= 3 \times 4 + 0. \end{aligned}$$

D'où $\mathrm{PGCD}(266, 224) = 14$. On résout donc l'équation :

$$266u + 224v = 14.$$

Par l'algorithme d'Euclide, on trouve :

$$\begin{aligned} 14 &= 224 - 5 \times 42 \\ 14 &= 224 - 5(266 - 244) \\ 14 &= 6 \times 224 - 5 \times 266. \end{aligned}$$

On obtient $u = -5$ et $v = 6$.

On peut montrer que toutes les solutions sont les couples :

$$\{(-5 + 224k, 6 - 266k), k \in \mathbb{Z}\}.$$

□

4.3 Décomposition en facteurs premiers et PGCD

THÉORÈME 4.9 (THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE). Pour tout $n \in \mathbb{N}^* \setminus \{1\}$.

1. Il existe k nombres premiers naturels, $p_1, \ldots, p_k$ distincts deux à deux et des nombres entiers non nuls $\alpha_1, \ldots, \alpha_k$ tels que :
$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$
2. Il y a unicité de cette décomposition à l'ordre des facteurs près.

Démonstration du théorème 4.9. ◊

Existence : La démonstration se fait par récurrence sur n.

Initialisation : Si $n = 2$ alors $n = 2^1$.

Hérédité : Si $n \geq 2$ alors n possède au moins un diviseur premier de p et l'on peut écrire $n = pm$ avec $m < n$. Si $m = 1$ alors c'est fini ! Sinon on applique l'hypothèse de récurrence à m pour obtenir la décomposition sur n.

Unicité : la démonstration de l'unicité se fait par récurrence sur n.

Initialisation : L'unicité est évidente pour $n = 2$. En effet, si $2 = q_1^{\beta_1} \cdots q_m^{\beta_m}$ montre que $q_i \mid 2$ pour tout $1 \leq i \leq m$, ce qui impose d'avoir $m = 1$, $q_1 = 2$ et $\beta_1 = 1$.

Hérédité : Si l'unicité est démontrée jusqu'au rang n, on suppose que :

$$n + 1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = q_1^{\beta_1} \cdots q_m^{\beta_m}$$

avec $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_m \in \mathbb{N}^*$ et où les $p_1, \ldots, p_k$ et $q_1, \ldots, q_m$ sont des nombres entiers.

$p_k \mid q_1^{\beta_1} \cdots q_m^{\beta_m}$ donc p_k divise l'un des q_i, par exemple $p_k \mid q_m$. Comme p_k est premier, cela entraîne que $p_k = q_m$ et :

$$\frac{n+1}{p_k} = p_1^{\alpha_1} \cdots p_k^{\alpha_k - 1} = q_1^{\beta_1} \cdots q_m^{\beta_m - 1}.$$

On applique l'hypothèse de récurrence à cette décomposition en distinguant deux cas :

1. Si $\alpha_k = 1$ alors $\beta_m = 1$ autrement q_m diviserait l'un des p_i avec $i \neq m$, ce qui est absurde.
2. Si $\alpha_k > 1$ alors $\beta_m > 1$ autrement p_k diviserait l'un des q_i avec $i \neq k$, ce qui est encore absurde.

□