Université de Tours
Licence 2 Mathématiques

TD 2 : PGCD

Arithmétique | Semestre 1

Exercice 1
Trouver le pgcd des paires de nombres suivants et l'exprimer comme une combinaison linéaire des nombres donnés :
$$(26, 19); \quad (187, 34); \quad (841, 160).$$

Solution. On a
$$\begin{aligned}26 &= 19 \times 1 + 7\\ 19 &= 7 \times 2 + 5\\ 7 &= 5 \times 1 + 2\\ 5 &= 2 \times 2 + 1\\ 2 &= 1 \times 2 + 0.\end{aligned}$$
Ainsi $\mathbf{pgcd}\,(26, 19) = 1$. De plus
$$\begin{aligned}1 &= 5 - 2 \times 2\\ &= 5 - 2 \times (7 - 5)\\ &= 3 \times 5 - 2 \times 7\\ &= 3 \times (19 - 2 \times 7) - 2 \times 7\\ &= 3 \times 19 - 8 \times 7\\ &= 3 \times 19 - 8 \times (26 - 19)\\ &= 11 \times 19 - 8 \times 26.\end{aligned}$$
On a
$$\begin{aligned}187 &= 5 \times 34 + 17\\ 34 &= 17 \times 2.\end{aligned}$$
Ainsi $\mathbf{pgcd}\,(187, 34) = 17$. De plus,
$$17 = 187 - 5 \times 34.$$
Enfin,
$$\begin{aligned}841 &= 5 \times 160 + 41\\ 160 &= 3 \times 41 + 37\\ 41 &= 37 + 4\\ 37 &= 4 \times 9 + 1,\end{aligned}$$
et donc $\mathbf{pgcd}\,(841, 160) = 1$. De plus,
$$\begin{aligned}1 &= 37 - 4 \times 9\\ &= 37 - 9 \times (41 - 37)\\ &= 10 \times 37 - 9 \times 41\\ &= 10 \times (160 - 3 \times 41) - 9 \times 41\\ &= 10 \times 160 - 39 \times 41.\end{aligned}$$
$\square$

Exercice 2
Soient $a, b \in \mathbb{Z}$ et $d = \mathbf{pgcd}\,(a, b)$. Démontrer les assertions suivantes :

1. Pour tout $m \in \mathbb{Z}$, $\mathbf{pgcd}\,(a, b + ma) = \mathbf{pgcd}\,(a, b)$.
2. Pour tout $m \in \mathbb{Z}$, $\mathbf{pgcd}\,(ma, mb) = |m| \times \mathbf{pgcd}\,(a, b)$.
3. $\mathbf{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Solution.

1. Soit $m \in \mathbb{Z}$. Notons $\delta = \mathbf{pgcd}\,(a, b + ma)$.
Par définition, d divise a et d divise b, donc d divise toute combinaison linéaire de a et b. En particulier, d divise
$$1 \times b + m \times a = b + ma.$$
Ainsi, d divise a et d divise $b + ma$. Par conséquent, d divise leur **pgcd**, c'est-à-dire d divise δ.
Réciproquement, par définition, δ divise a et δ divise $b+ma$, donc δ divise toute combinaison linéaire de a et $b + ma$. En particulier, δ divise
$$1 \times (b + ma) + (-m) \times a = b.$$
Ainsi, δ divise a et δ divise b. Par conséquent, δ divise leur **pgcd**, c'est-à-dire δ divise d.
Ceci prouve que $d = \delta$.
2. Soit $m \in \mathbb{Z}$. Pour fixer les idées, supposons que $m > 0$. Notons $\delta = \mathbf{pgcd}\,(ma, mb)$.
Par définition, d divise a et b donc md divise ma et mb. Ainsi, md divise δ :
$$\exists k \in \mathbb{Z}, \quad \delta = k(md).$$
Pour conclure, on va montrer que $k = 1$. Comme $k(md)$ divise ma et mb et comme $m > 0$, on en déduit que kd divise a et b, et donc kd divise leur **pgcd**, c'est-à-dire que kd divise d.
Ceci implique que $k = 1$. Ensuite, si $m < 0$, alors $-m > 0$ et donc
$$\mathbf{pgcd}\,(ma, mb) = \mathbf{pgcd}\,(-ma, -mb) = (-m) \times \mathbf{pgcd}\,(a, b) = |m| \times \mathbf{pgcd}\,(a, b)\,.$$
3. On utilise la question précédente :
$$d = \mathbf{pgcd}\,(a, b) = \mathbf{pgcd}\left(d \times \frac{a}{d}, d \times \frac{b}{d}\right) = d \times \mathbf{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right).$$
En simplifiant par d, on trouve que
$$1 = \mathbf{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right).$$

□

Exercice 3 (Vrai ou faux ?)
Soient $a, b \in \mathbb{Z}$ et $d \in \mathbb{N}^*$. Les assertions suivantes sont-elles vraies ou fausses ? Justifier.

1. Si d divise $\mathbf{pgcd}\,(a, b)$, alors d divise a et d divise b.
2. Si d divise $a + b$, alors d divise $\mathbf{pgcd}\,(a, b)$.
3. Si d divise ab, alors d divise a ou d divise b.
4. Pour tout $m \in \mathbb{Z}$, $\mathbf{pgcd}\,(a, a + bm) = \mathbf{pgcd}\,(a, b)$.
5. Si $\mathbf{pgcd}\,(a, b) = 1$, alors $\mathbf{pgcd}\,(a, a + b) = 1$ et $\mathbf{pgcd}\,(b, a + b) = 1$.

Solution.

1. C'est vrai bien sûr, par transitivité de la divisibilité. Comme $\mathbf{pgcd}\,(a,b)$ divise a et b, si d divise $\mathbf{pgcd}\,(a,b)$, alors d divise a et d divise b.
2. C'est faux. Posons $a=9$, $b=3$ et $d=4$. Alors d divise $a+b=12$, mais d ne divise pas $\mathbf{pgcd}\,(a,b)=3$.
3. C'est faux encore.. Posons $a=4$, $b=3$ et $d=6$. Alors d divise $ab=12$ mais d ne divise pas a et d ne divise pas b.
4. C'est faux encore... Posons $m=2$, $a=2$, $b=3$. Alors
$$\mathbf{pgcd}\,(a,a+bm)=\mathbf{pgcd}\,(2,8)=2\neq 1=\mathbf{pgcd}\,(2,3)=\mathbf{pgcd}\,(a,b)\,.$$
5. Cette assertion est vraie. On propose deux rédactions.

   Méthode 1 (avec Bézout). Comme a et b sont premiers entre eux, d'après l'identité de Bézout,
$$\exists u,v\in\mathbb{Z},\quad au+bv=1.$$
   Alors,
$$1=au+bv=au+bv+av-av=a(u-v)+(a+b)v.$$
   Ceci prouve que a et $a+b$ sont premiers entre eux. Bien sûr, on montre de manière similaire que b et $a+b$ sont premiers entre eux.

   Méthode 2 (élémentaire). Soit d un diviseur commun de a et $a+b$. Pour montrer que a et $a+b$ sont premiers entre eux, il suffit de montrer que $d=\pm1$. Comme d divise a et $a+b$, d divise toute combinaison linéaire de a et $a+b$. En particulier, d divise $(a+b)-a$, c'est-à-dire b. Bref, d divise a et d divise b, donc d divise $\mathbf{pgcd}\,(a,b)=1$. Ainsi, $d=\pm1$, donc a et $a+b$ sont premiers entre eux. On montre de manière similaire que b et $a+b$ sont premiers entre eux.

□

Exercice 4* (PGCD et Bézout)
Soient a et b deux entiers.

1. (a) Montrer que si
$$\exists x,y\in\mathbb{Z},\quad ax+by=1,$$
   alors a et b sont premiers entre eux.

   (b) Montrer que la réciproque est vraie. *Indication : on pourra montrer que l'ensemble*
$$\mathbf{E}=\{ax+by\mid x,y\in\mathbb{Z}\}\cap\mathbb{N}^*$$
   admet un plus petit élément.
2. Soit $d\in\mathbb{N}^*$. Montrer que
$$d=\mathbf{pgcd}\,(a,b)\implies\exists x,y\in\mathbb{Z},\quad ax+by=d.$$
   Que dire de la réciproque ?
3. Soit $d\in\mathbb{Z}$. Que dire de l'assertion :
$$(a\mid d\quad\text{et}\quad b\mid d)\implies ab\mid d.$$
   Et si a et b sont premiers entre eux ?

Solution.

1. (a) Soit d un diviseur commun de a et b. Comme d divise a et b, d divise toute combinaison linéaire de a et b. En particulier, d divise $ax+by=1$, donc $d=\pm1$. Ceci prouve que a et b sont premiers entre eux.

(b) On suit l'indication. L'ensemble $\mathbf{E}$ est non vide puisqu'il contient par exemple a^2 et b^2. C'est donc un sous-ensemble de $\mathbb{N}^*$ non vide : il admet un plus petit élément qu'on note $d \in \mathbf{E}$. L'objectif est donc de montrer que $d = 1$.
Comme d est un élément de $\mathbf{E}$, il existe $x_0, y_0 \in \mathbb{Z}$ tel que

$$d = ax_0 + by_0.$$

La division euclidienne de a par d donne :

$$a = d \times q, \quad q \in \mathbb{Z},\ 0 \leq r < d.$$

L'entier positif r vérifie donc

$$r = a - dq = a(1 - qx_0) + b(-qy_0).$$

Il est nécessairement nul par minimalité de d. Ainsi, $r = 0$ et donc d divise a. De même, on montre que d divise b. On en déduit que d divise $\mathbf{pgcd}\,(a, b) = 1$, donc $d = 1$.

2. En utilisant l'exercice 2, on peut dire que

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

D'après la question précédente,

$$\exists x, y \in \mathbb{Z}, \quad \frac{a}{d} \times x + \frac{b}{d} \times y = 1.$$

On multiplie tout par d pour obtenir que

$$ax + by = d.$$

La réciproque est fausse. Posons par exemple $a = 10$ et $b = 15$. Alors on a

$$4 \times 10 - 2 \times 15 = 10,$$

pourtant $\mathbf{pgcd}\,(10, 15) = 5 \neq 10$.

3. Cette assertion est fausse ! Posons $a = 4$, $b = 6$ et $d = 12$. Alors a divise d, b divise b, pourtant ab ne divise pas d.
Par contre, si en plus, a et b sont premiers entre eux, le résultat est vrai. En effet, comme a et b divisent d, on peut écrire :

$$d = \alpha \times a; \quad d = \beta \times b; \quad \alpha, \beta \in \mathbb{Z}.$$

De plus, comme a et b sont premiers entre eux,

$$\exists u, v \in \mathbb{Z}, \quad au + bv = 1.$$

On multiplie cette égalité par d et on utilise les hypothèses de divisibilité :

$$d = aud + bvd = au(\beta \times b) + bv(\alpha \times a) = ab \times (u\beta + v\alpha),$$

ce qui prouve que ab divise d.

□