♦ Chapitre 4 : PGCD et applications

I. — PGCD

1) Définition

Définition 1

Si a et b sont deux entiers, on note $\mathcal{D}(a)$ l'ensemble des diviseurs positifs de a et $\mathcal{D}(a,b)$ l'ensemble des diviseurs positifs communs à a et b. Autrement dit, $\mathcal{D}(a) = \{n \in \mathbb{N} \,|\, n|a\}$ et $\mathcal{D}(a,b) = \{n \in \mathbb{N} \,|\, n|a \text{ et } n|b\}$.

Exemple 2. $\mathcal{D}(15) = \{1,3,5,15\}$, $\mathcal{D}(27) = \{1,3,9,27\}$ et $\mathcal{D}(15,27) = \{1,3\}$.

Propriété 3

Soit a et b deux entiers. Alors,

1. $\mathcal{D}(a,b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.
2. $1 \in \mathcal{D}(a,b)$ et donc $\mathcal{D}(a,b) \neq \varnothing$.
3. Si a ou b est non nul, $\mathcal{D}(a,b)$ est un ensemble fini.
4. Si a divise b alors $\mathcal{D}(a,b) = \mathcal{D}(a)$. En particulier, $\mathcal{D}(a,0) = \mathcal{D}(a)$.
5. $\mathcal{D}(a,b) = \mathcal{D}(|a|,|b|)$.

Démonstration.

1. Soit $n \in \mathbb{N}$. Alors,
$$n \in \mathcal{D}(a,b) \Leftrightarrow n \mid a \text{ et } n \mid b \Leftrightarrow n \in \mathcal{D}(a) \text{ et } n \in \mathcal{D}(b) \Leftrightarrow n \in \mathcal{D}(a) \cap \mathcal{D}(b).$$
Ainsi, $\mathcal{D}(a,b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.
2. On sait que 1 divise tout entier donc $1 \in \mathcal{D}(a,b)$.
3. Supposons que a est non nul. Alors, $\mathcal{D}(a,b) = \mathcal{D}(a) \cap \mathcal{D}(b) \subset \mathcal{D}(a)$ et, comme $a \neq 0$, on sait que $\mathcal{D}(a)$ est fini. Il s'ensuit que $\mathcal{D}(a,b)$ est fini. On raisonne de même si $b \neq 0$.
4. Si a divise b alors, par transitivité de la relation *divise*, tout diviseur de a et un diviseur de b donc $\mathcal{D}(a) \subset \mathcal{D}(b)$. Dès lors, $\mathcal{D}(a,b) = \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a)$.
De plus, quelle que soit la valeur de a, a divise 0 donc $\mathcal{D}(a,0) = \mathcal{D}(a)$.
5. On sait que $\mathcal{D}(a) = \mathcal{D}(|a|)$ et $\mathcal{D}(b) = \mathcal{D}(|b|)$ donc
$$\mathcal{D}(a,b) = \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(|a|) \cap \mathcal{D}(|b|) = \mathcal{D}(|a|,|b|).$$

□

Théorème et définition 4

Soit a et b deux entiers non tous les deux nuls. Alors, $\mathcal{D}(a,b)$ admet un plus grand élément d. L'entier d est appelé le plus grand commun diviseur de a et b et on le note $d = \text{PGCD}(a,b)$ ou $d = a \wedge b$.

Démonstration. Comme au moins un des deux nombres a ou b n'est pas nul, $\mathcal{D}(a,b)$ est fini. Ainsi, $\mathcal{D}(a,b)$ est une partie finie et non vide de $\mathbb{N}$ donc $\mathcal{D}(a,b)$ admet une plus grand élément. □

Remarque 5. Par définition, $\text{PGCD}(a,b)$ est le plus grand entier positif qui divise à la fois a et b. De plus, comme $1 \in \mathcal{D}(a,b)$, $\text{PGCD}(a,b) \geqslant 1$.

Exemple 6. Comme $\mathcal{D}(15,27) = \{1,3\}$, $\text{PGCD}(15,27) = 3$.

Exercice 7. Soit $n \in \mathbb{N}$. Déterminer le P.G.C.D. de $a_n = 2n+3$ et $b_n = 3n+4$.

Solution. Notons $d_n = \text{PGCD}(a_n, b_n)$. Alors, d_n divise a_n et b_n donc d_n divise tout combinaison linéaire à a_n et b_n. En particulier, d_n divise $3a_n - 2b_n = 3(2n+3) - 2(3n+4) = 1$. De plus, $d_n \geqslant 1$ donc $d_n = 1$.

Propriété 8

Soit a et b deux entiers nous tous les deux nuls.

1. Si $a \neq 0$ et si a divise b alors $\text{PGCD}(a,b) = |a|$. En particulier, pour tout $a \neq 0$, $\text{PGCD}(a,0) = |a|$.
2. S'il existe un entier strictement positif d tel que $\mathcal{D}(a,b) = \mathcal{D}(d)$ alors $\text{PGCD}(a,b) = d$.
3. $\text{PGCD}(a,b) = \text{PGCD}(|a|, |b|)$.

Démonstration.

1. Si a divise b alors $\mathcal{D}(a,b) = \mathcal{D}(a)$ et le plus grand élément de $\mathcal{D}(a)$ est $|a|$ car $a \neq 0$.
2. S'il existe un entier strictement positif d tel que $\mathcal{D}(a,b) = \mathcal{D}(d)$ alors, comme le plus grand élément de $\mathcal{D}(d)$ est d (car $d > 0$), le plus grand élément de $\mathcal{D}(a,b)$ est aussi d.
3. Cela provient immédiatement du fait que $\mathcal{D}(a,b) = \mathcal{D}(|a|, |b|)$.

□

Remarque 9. — Les propriétés 1 et 3 ci-dessus montrent que, pour la recherche d'un PGCD, on peut se restreindre au cas de deux entiers strictement positifs.

2) Algorithme d'Euclide (ou algorithme des divisions successives)

Dans tout ce paragraphe, a et b désignent des entiers naturels tels que $0 < b < a$. On note $d = \text{PGCD}(a,b)$.

Lemme 10 : Lemme d'Euclide

Si r désigne le reste dans la division euclidienne de a par b alors $\mathcal{D}(a,b) = \mathcal{D}(b,r)$ et donc, en particulier, $d = \text{PGCD}(b,r)$.

Démonstration. Notons r le reste de a dans la division euclidienne par b. Alors, il existe un entier q tel que $a = bq + r$.

Soit $n \in \mathcal{D}(b,r)$. Alors, n divise b et r donc n divise $bq + r$ i.e. n divise a. Ainsi, n divise a et b donc $n \in \mathcal{D}(a,b)$. On en déduit que $\mathcal{D}(b,r) \subset \mathcal{D}(a,b)$.

Inversement, soit $n \in \mathcal{D}(a,b)$. Alors, n divise a et b donc n divise $a - bq$ i.e. n divise r. Ainsi, n divise b et r donc $n \in \mathcal{D}(b,r)$. On en déduit que $\mathcal{D}(a,b) \subset \mathcal{D}(b,r)$.

On conclut donc que $\mathcal{D}(a,b) = \mathcal{D}(b,r)$. □

Algorithme d'Euclide ou des divisions successives

Posons $r_0 = b$ et r_1 le reste dans la division de a par $r_0 = b$. Alors, d'après le lemme d'Euclide, $d = \text{PGCD}(r_0, r_1)$. Deux cas sont possibles,

— si $r_1 = 0$ alors $d = \text{PGCD}(r_0, r_1) = \text{PGCD}(r_0, 0) = r_0$ et on s'arrête.
— sinon, $r_1 > 0$ et on peut effectuer la division euclidienne de r_0 par r_1, ce qui nous donne un reste r_2 et on est recommence le processus pour trouver $\text{PGCD}(r_1, r_2)$ qui d'après le lemme d'Euclide est égal d.

On est sûr que l'algorithme s'arrête en un nombre fini d'étapes car la suite de restes $r_0 > r_1 > r_2 > ...$ est une une suite strictement décroissante d'entiers naturels donc elle s'annule au maximum au bout de $r_0 = b$ étapes.

Ainsi, il existe un reste $r_k \neq 0$ tel que $r_{k+1} = 0$. Or, par le lemme d'Euclide,

$$\mathcal{D}(a, b) = \mathcal{D}(r_0, r_1) = \mathcal{D}(r_1, r_2) = \cdots = \mathcal{D}(r_k, r_{k+1})$$

donc $\mathcal{D}(a, b) = \mathcal{D}(r_k)$ car $r_{k+1} = 0$.

On en déduit en particulier que le plus grand élément de $\mathcal{D}(a, b)$ est r_k. Autrement dit, on a montré la propriété suivante.

Propriété 11

Le P.G.C.D. de a et b est le dernier reste non nul dans l'algorithme d'Euclide.

Exemple 12. — Déterminer $\text{PGCD}(1636, 1128)$.

On écrit les divisions successives :

$$\begin{aligned}
1636 &= 1 \times 1128 + 508 \\
1128 &= 2 \times 508 + 112 \\
508 &= 4 \times 112 + 60 \\
112 &= 1 \times 60 + 52 \\
60 &= 1 \times 52 + 8 \\
52 &= 6 \times 8 + \boxed{4} \\
8 &= 2 \times 4 + 0
\end{aligned}$$

Le dernier reste non nul est 4 donc $\text{PGCD}(1128, 508) = 4$.

Remarque 13. L'algorithme d'Euclide se programme facilement en Python :

```
def pgcd(a,b):
    while (b!=0):
        r=a%b
        a=b
        b=r
    return(a)
```

On remarquera que ce programme fonctionne même si $b > a$ ou si a ou b est nul.

Corollaire 14

L'ensemble des diviseurs communs positifs de a et b est l'ensemble des diviseurs positifs de d i.e. $\mathcal{D}(a, b) = \mathcal{D}(d)$.

Démonstration. On a vu précédemment que $\mathcal{D}(a, b) = \mathcal{D}(r_k)$ où $r_k = d$ est le P.G.C.D. de a et b donc l'ensemble des diviseurs positifs communs à a et b est l'ensemble des diviseurs de d. □

II. — Théorème de Bézout

Définition 15

— On dit que deux entiers non tous nuls a et b sont premiers entre eux si $a \wedge b = 1$. (On dit aussi que a est premier avec b ou que b est premier avec a.)

Exemple 16. — Les entiers 12 et 35 sont premiers entre eux car $\mathcal{D}(12) = \{1, 2, 3, 4, 6, 12\}$ et $\mathcal{D}(35) = \{1, 5, 7, 35\}$ donc $\text{PGCD}(12, 35) = 1$.

Théorème 17. — Théorème de Bézout

Deux entiers non tous les deux nuls a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que $au + bv = 1$.

L'égalité $au + bv = 1$ est alors appelée *identité de Bézout*.

Démonstration. Soit a et b deux entiers non tous les deux nuls.

Supposons qu'il existe deux entiers u et v tels que $au + bv = 1$. Notons $d = a \wedge b$. Alors, $d|a$ et $d|b$ donc d divise $au + bv$ i.e. d divise 1. Comme $d > 0$, on en déduit que $d = 1$ i.e. a et b sont premiers entre eux.

Réciproquement, supposons que a et b sont premiers entre eux. Notons E l'ensemble des entiers strictement positifs de la forme $au + bu$ i.e. $E = \{m \in \mathbb{N}^* \mid \exists (u, v) \in \mathbb{Z}^2,\ m = au + bv\}$. Comme a et b ne sont pas tous les deux nuls, par exemple $a \neq 0$. Si $a > 0$ alors $a \in E$ car $a = a \times 1 + b \times 0$ et $a > 0$ et si $a < 0$ alors $-a \in E$ car $-a = a \times (-1) + b \times 0$ et $-a > 0$. Ainsi, E est une partie non vide de $\mathbb{N}$. Elle admet donc un plus petit élément p. Comme $p \in E$, $p > 0$ et il existe $(u, v) \in \mathbb{Z}^2$ tel que $p = au + bv$.

Effectuons la division euclidienne de a par p : il existe $(q, r) \in \mathbb{Z}^2$ tel que $a = pq + r$ avec $0 \leq r < p$. Ainsi, $a = (au + bv)q + r$ donc $r = (1 - uq)a + b(-vq)$ i.e. r est de la forme $r = aU + bV$ où $U = 1 - uq$ et $V = -vq$ sont des entiers. Comme $r < p$ et p est minimal dans E, on en déduit que $r \neq E$ donc $r \notin \mathbb{N}^*$ i.e. $r \leqslant 0$. Mais, par définition, $r \geqslant 0$ donc $r = 0$. Ainsi, p divise a.

On démontre de même que p divise b.

Dès lors, p est un diviseur positif commun à a et b donc p divise $a \wedge b$ (d'après le corollaire 14). Or, $a \wedge b = 1$ et $p > 0$ donc $p = 1$. On conclut que $au + bv = 1$ donc il existe deux entiers u et v tels que $au + bv = 1$. □

Exemple 18.

1. $33 \times 11 + (-1) \times 32 = 1$ donc, d'après le théorème de Bézout, 11 et 32 sont premiers entre eux.
2. Pour tout entier $n \in \mathbb{N}$, $(n + 1) - n = 1$ donc, d'après le théorème de Bézout, n et $n + 1$ sont premiers entre eux.
3. Justifier l'existence et déterminer deux entiers u et v tels que $257u + 124v = 1$.
   Écrivons les divisions successives :

$$\begin{aligned} (D_1)&\quad 257 = 2 \times 124 + 9 \\ (D_2)&\quad 124 = 13 \times 9 + 7 \\ (D_3)&\quad 9 = 1 \times 7 + 2 \\ (D_4)&\quad 7 = 3 \times 2 + \boxed{1} \end{aligned}$$

   On trouve un reste égal à 1, ce n'est pas nécessaire d'effectuer la division suivante car le reste sera nécessairement nul. Ainsi, le P.G.C.D. de 257 et 124 est égal à 1 i.e. 257 et 124

sont premiers entre eux. D'après le théorème de Bézout, il existe donc deux entiers u et v tels que $257u + 124v = 1$.

Pour déterminer deux tels entiers, nous allons « remonter » l'algorithme d'Euclide.

Partant de (D_4), on peut écrire $1 = 7 - 3 \times 2$. Or, grâce à (D_3), $2 = 9 - 7$ donc, en substituant, on obtient

$$1 = 7 - 3 \times (9 - 7) = 7 - 3 \times 9 + 3 \times 7 = 4 \times 7 - 3 \times 9.$$

Ensuite, grâce à (D_2), on peut écrire $7 = 124 - 13 \times 9$ donc

$$1 = 4(124 - 13 \times 9) - 3 \times 9 = 4 \times 124 - 52 \times 9 - 3 \times 9 = 4 \times 124 - 55 \times 9.$$

Enfin, grâce à (D_1), on a $9 = 257 - 2 \times 124$ donc

$$1 = 4 \times 124 - 55(257 - 2 \times 124) = 4 \times 124 - 55 \times 257 + 110 \times 124 = 114 \times 124 - 55 \times 257.$$

Ainsi, $124 \times 114 + 257 \times (-55) = 1$ donc $u = 114$ et $v = -55$ conviennent.

Remarque 19.

1. Les entiers u et v tels que $au + bv = 1$ sont premiers entre eux d'après le théorème de Bézout.
2. Les entiers $u$et v tels que $au + bv = 1$ ne sont pas uniques. Par exemple, $3 \times 1 + 2 \times (-1) = 3 \times 3 + 2 \times (-4) = 1$.

Théorème 20

Soit a et b deux entiers non tous les deux nuls et d un entier strictement positif. Les propositions suivantes sont équivalentes :

1. $d = a \wedge b$;
2. d divise a, d divise b et les entiers $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ sont premiers entre eux ;
3. d divise a, d divise b et il existe deux entiers u et v tels que $au + bv = d$.

Démonstration.

$\underline{\mathbf{1} \Rightarrow \mathbf{2}}$. On suppose que $d = a \wedge b$. Par définition, d divise a et d divise b et ainsi $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ sont des entiers. Notons $\delta = a' \wedge b'$. Alors, δ divise a' et b' donc $d\delta$ divise da' et db' i.e. $d\delta$ divise a et $d\delta$ divise b. Par le corollaire 14, $d\delta$ est donc un diviseur de $a \wedge b = d$ et donc, comme $d > 0$, $d\delta \leqslant d$. En divisant par $d > 0$, on en déduit que $\delta \leqslant 1$ et, par ailleurs, $\delta \geqslant 1$ donc $\delta = 1$. Ainsi, a' et b' sont premiers entre eux.

$\underline{\mathbf{2} \Rightarrow \mathbf{3}}$. Supposons que d divise a, d divise b et que les entiers $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ sont premiers entre eux. Alors, par le théorème de Bézout, il existe deux entiers u et v tels que $a'u + b'v = 1$. En multipliant par d, il vient $da'u + db'v = d$ i.e. $au + bv = 1$.

$\underline{\mathbf{3} \Rightarrow \mathbf{1}}$. Supposons que d divise a, d divise b et qu'il existe deux entiers u et v tels que $au + bv = d$. Notons $D = a \wedge b$. Comme d divise a et d divise b, d'après le corollaire 14, d divise D. Mais, comme D divise a et D divise b, D divise $au + bv$ i.e. D divise d. Comme D et d sont positifs, on en déduit que $d = D$. □

Remarque 21. ATTENTION ! Ce n'est pas parce qu'il existe deux entiers u et v tels que $au + bv = d$ que $d = a \wedge b$. Par exemple, $3 \times 2 + 2 \times (-2) = 2$ or $3 \wedge 2 = 1$.

Corollaire 22

Soit a, b et k trois entiers naturels non nuls. Alors,

1. $\text{PGCD}(ka, kb) = k\text{PGCD}(a, b)$.
2. Si b et k sont premiers entre eux alors $\text{PGCD}(ka, b) = \text{PGCD}(a, b)$.

Démonstration. Notons $d = a \wedge b$.

1. Comme d divise a et d divise b, kd divise ka et kb. De plus, par le théorème 20, il existe deux entiers u et v tels que $au+bv = d$. Mais alors, en multipliant par k, $(ka)u+(kb)v = kd$ donc grâce au théorème 20 que $\text{PGCD}(ka, kb) = kd$.
2. Comme d divise a et d divise b, d divise ka et b. De plus, comme précédemment, il existe deux entiers u et v tels que $au + bv = 1$ et, comme $b \wedge k = 1$, par le théorème de Bézout, il existe deux entiers x et y tels que $bx + ky = 1$. En multipliant membre à membre ces égalités, il vient $(au + bv)(bx + ky) = d$ donc $(ka)(uy) + b(aux + bvx + vky) = d$. Ainsi, en posant $U = uy$ et $V = aux + bvx + vky$, il existe deux entiers U et V tels que $(ka)U + bV = d$. Par le théorème 20, on conclut que $\text{PGCD}(ka, b) = 1$.

□

Exemple 23. Soit m et n deux entiers naturels non nuls. Déterminer le P.G.C.D. de mn et de $(2m + 1)n$.

Solution. Commençons par remarquer que $\text{PGCD}(mn, (2m + 1)n) = n\text{PGCD}(m, 2m + 1)$. De plus, $2m + 1 - 2 \times m = 1$ donc, par le théorème de Bézout, $\text{PGCD}(2m + 1, m) = 1$ et on conclut que $\text{PGCD}(mn, (2m + 1)n) = n$.

III. — Théorème de Gauss

1) Théorème de Gauss

Théorème 24. — Théorème de Gauss

Soit a, b et c trois entiers. Si a divise bc et si a et premier avec b alors a divise c.

Démonstration. Supposons que a divise bc et que $a \wedge b = 1$. Alors, par le théorème de Bézout, il existe deux entiers u et v tels que $au + bv = 1$. Multiplions cette dernière égalité par c. Il vient $auc + bvc = c$ i.e. . Or, a divise bc et a divise a donc a divise $a(uc) + (bc)$ i.e. a divise c. □

Exemple 25. Déterminer l'ensemble des couples d'entiers (a, b) tels que $3a = 5b$.

Solution. Supposons que a et b sont deux entiers tels que $3a = 5b$. Alors, 5 divise $3a$ et, comme $2 \times 3 - 5 = 1$, 3 et 5 sont premiers entre eux donc, par le théorème de Gauss, 5 divise a. Ainsi, il existe un entier k tel que $a = 5k$. Dès lors, $3(5k) = 5b$ i.e. $3k = b$. Ainsi, on a montré que si $(a\,;b)$ d'entiers tels que $3a = 5b$ alors il existe un entier k tel que $a = 5k$ et $b = 3k$.

Réciproquement, soit $k \in \mathbb{Z}$. Posons $a = 5k$ et $b = 3k$. Alors, $3a = 3(5k) = 5(3k) = 5b$.

Ainsi, l'ensemble cherché est $\{(5k\,;3k) \mid k \in \mathbb{Z}\}$.

Corollaire 26

Soit a, b et c trois entiers. Si a divise c, b divise c et si a et b sont premiers entre eux alors ab divise c.

Démonstration. Supposons que a divise c, b divise c et que a et b sont premiers entre eux. Alors, il existe deux entiers k et k' tels que $c = ka = k'b$. Ainsi, a divise $k'b$. Or, $a \wedge b = 1$ donc, par le théorème de Gauss, a divise k'. Ainsi, il existe un entier q tel que $k' = qa$. Alors, $c = k'b = (qa)b = q(ab)$ donc ab divise c. □

Exemple 27. Soit $n \in \mathbb{N}$ et $A_n = n(n+1)(n+2)(n+3)(n+4)$. Démontrer que A_n est un multiple de 120.

Solution Remarquons que $120 = 8 \times 3 \times 5$.

Comme n, $n+1$ et $n+2$ sont trois entiers consécutifs, l'un deux est divisible par 3 donc $n(n+1)(n+2)$ est un multiple de 3 et ainsi $3 \mid A_n$.

De même, n, $n+1$, $n+2$, $n+3$ et $n+4$ sont cinq entiers consécutifs donc l'un deux est divisible par 3 et ainsi A_n divisible par 5.

Comme 5 et 3 sont premiers entre eux, on déduit du théorème de Gauss que $3 \times 5 = 15$ divise A_n.

Enfin, remarquons que n, $n+1$, $n+2$ et $n+3$ sont quatre entiers consécutifs donc l'un deux est divisible par 4 et un autre est pair donc le produit est divisible par 8. Comme 8 et 15 sont premiers entre eux (car $2 \times 8 - 15 = 1$), on conclut, grâce au théorème de Gauss, que $120 = 8 \times 15$ divise A_n.

Autre méthode. Une autre méthode consiste à remarquer que $120 = 5!$ que

$$\frac{A_n}{5!} = \frac{n(n+1)(n+2)(n+3)(n+4)}{5!} = \frac{(n-1)! \times n(n+1)(n+2)(n+3)(n+4)}{5! \times (n-1)!}$$
$$= \frac{(n+4)!}{5!(n-1)!} = \binom{n+5}{n}$$

donc $\dfrac{A_n}{5!}$ est un entier i.e. 5! divise A_n.

2) Fractions irréductibles

Définition 28

Un réel x est un nombre rationnel s'il existe deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ tel que $x = \frac{a}{b}$.
L'ensemble des nombres rationnels se note $\mathbb{Q}$.

Définition 29

Soit $(a\,;b) \in \mathbb{Z} \times \mathbb{N}^*$. On dit que la fraction $\frac{a}{b}$ est irréductible si $a \wedge b = 1$.

Propriété 30

Tout rationnel peut s'écrire de manière unique sous la forme d'une fraction irréductible.

Démonstration. Soit $r \in \mathbb{Q}$. Alors, il existe deux entiers a et b avec $b > 0$ tels que $r = \frac{a}{b}$. Notons $d = a \wedge b$. Par le théorème 20, il existe deux entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$ et donc $r = \frac{a'}{b'}$ est une écriture sous forme irréductible de r.

Supposons que r admette une autre écriture sous forme de fraction irréductible $r = \frac{\alpha}{\beta}$ où α et β sont des entiers premiers entre eux avec $\beta > 0$. Alors, $\frac{a'}{b'} = \frac{\alpha}{\beta}$ donc $a'\beta = \alpha b'$ et, en particulier, b' divise $a'\beta$. Or, b' est premier avec a' donc $b-$ divise β. On montre de même que β divise b' donc, comme β et b' sont positifs, $\beta = b'$. Dès lors, $a'\beta = \alpha' = \alpha\beta$ donc en divisant par $\beta > 0$, $a' = \alpha$. Ainsi, l'écriture est bien unique. □

Corollaire 31

$\sqrt{2}$ n'est pas rationnel.

Démonstration. Raisonnons par l'absurde en supposant que $\sqrt{2} \in \mathbb{Q}$. Alors, il existe deux entiers a et b premiers entre eux tels que $\sqrt{2} = \frac{a}{b}$ i.e. $a = b\sqrt{2}$. En élevant au carré, on en déduit que $a^2 = 2b^2$. Ainsi, a^2 est pair et donc a est pair. Il existe un entier k tel que $a = 2k$ donc $2b^2 = a^2 = (2k)^2 = 4k^2$ et ainsi $b^2 = 2k^2$. Dès lors, b^2 est pair donc b est également pair. Ainsi, a et b sont tous les deux divisibles par 2 ce qui est absurde car ils sont premiers entre eux.

On conclut que $\sqrt{2}$ n'est pas un nombre rationnel. □

3) L'équation diophantienne $ax + by = c$

On considère trois entiers a, b et c. On note $d = a \wedge b$ et (E) l'équation

$$\text{(E) } ax + by = c$$

d'inconnue $(x, y) \in \mathbb{Z}^2$. Une telle équation est appelée une équation diophantienne. (De manière générale, une équation diophantienne est une équation dont les inconnues sont des entiers.)

Propriété 32

L'équation (E) possède des solutions si et seulement si d divise c.

Démonstration. Supposons que (E) possède des solutions. Alors, il existe deux entiers u et v tels que $au + bv = c$. Or, d divise a et d divise b donc d divise $au + bv$ et donc d divise c.

Réciproquement, supposons que d divise c. Alors, il existe un entier k tel que $c = dk$. Comme $d = a \wedge b$, par le théorème 20, il existe deux entiers u et v tels que $au + bv = d$. En multipliant par k, il vient $auk + bvk = kd$ i.e. $a(uk) + b(vk) = c$ et donc $(x, y) = (uk, vk)$ est une solution de (E) dans $\mathbb{Z}^2$. □

Exemple 33. — Résoudre dans $\mathbb{Z}^2$ l'équation (E) : $24x + 18y = 36$.

Méthode

1. Existence de solution et réduction à des coefficients premiers entre eux
   Le PGCD de 24 et 18 est 6 (car $24 = 6 \times 4$ et $18 = 6 \times 3$ avec $4 \wedge 3 = 1$) et 6 divise 36 donc (E) a des solutions et (E) équivaut à (E') : $4x + 3y = 6$.
2. Recherche d'une solution particulière de (E')
   On a ici une solution évidente de $4x + 3y = 1$ qui est $(x\,;y) = (1\,;-1)$ donc $(6\,;-6)$ est une solution particulière que (E').
   Dans le cas général, on sait qu'on peut toujours trouver une solution particulière de (E') en « remontant » l'algorithme d'Euclide.
3. Recherche des solutions de (E')
   Supposons que $(u\,;v)$ est une solution de (E'). Alors, $4u + 3v = 6$ donc $4u + 3v = 4 \times 6 + 3 \times (-6)$ i.e. $4(u-6) = 3(-v-6)$. Ainsi, 3 divise $4(u-6)$ mais, comme $3 \wedge 4 = 1$, d'après le théorème de Gauss, 3 divise $u-6$. Ainsi, il existe un entier k tel que $u-6 = 3k$ i.e. $u = 3k+6$. De plus, comme $4(u-6) = 3(-v-6)$, $4 \times 3k = 3(-v-6)$ donc $4k = -v-6$ i.e. $v = -4k-6$. Ainsi, les solutions de (E') sont de la forme $(3k+6, -4k-6)$ avec $k \in \mathbb{Z}$.
   Réciproquement, soit $k \in \mathbb{Z}$. Alors, $4(3k+6) + 3(-4k-6) = 12k + 24 - 12k - 18 = 6$ donc $(3k+6, -4k-6)$ est solution de (E').

4. Conclusion

Ainsi, l'ensemble des solutions de (E') et donc de (E) est $\{(3k+6, -4k-6) \mid k \in \mathbb{Z}\}$.

Exercice 34. Déterminer l'ensemble S des entiers relatifs n tels que

$$\begin{cases} n \equiv 3 \quad [7] \\ n \equiv 5 \quad [13] \end{cases}.$$

Solution. Soit $n \in S$. Alors, il existe deux entiers p et q tels que $n = 3 + 7p$ et $n = 5 + 13q$. Ainsi, $3 + 7p = 5 + 13q$ donc $7p - 13q = 2$. Ainsi, $(p\,;q)$ est solution de l'équation diophantienne (E) : $7x - 13y = 2$. Étant donné que $2 \times 7 - 13 \times 1 = 1$, 7 et 13 sont premiers entre eux d'après le théorème de Bézout. De plus, $(2\,;1)$ est solution de l'équation $7x - 13y = 1$ donc, en multipliant par 2, le couple $(4\,;2)$ est une solution de (E).

Soit $(u\,;v)$ une solution de (E). Alors, $7u - 13v = 2$ donc $7u - 13v = 7 \times 4 - 13 \times 2$ i.e. $7(u-4) = 13(v-2)$. Ainsi, 13 divise $7(u-4)$ mais, comme $7 \wedge 13 = 1$, d'après le théorème de Gauss, 13 divise $u - 4$. Ainsi, il existe un entier k tel que $u - 4 = 13k$ i.e. $u = 13k + 4$. De plus, comme $7(u-4) = 13(v-2)$, $7 \times 13k = 13(y-2)$ donc $7k = v - 2$ i.e. $v = 7k + 2$. Ainsi, les solutions de (E) sont de la forme $(13k + 4, 7k + 2)$ avec $k \in \mathbb{Z}$.

On en déduit qu'il existe un entier k tel que $n = 3 + 7(13k + 4) = 91k + 31$.

Réciproquement, si $k \in \mathbb{Z}$ alors $91k+31 = 7(13k+4)+3 \equiv 3$ [7] et $91k+31 = 13(7k+2)+5 \equiv 5$ [13] donc $91k + 31 \in S$. On conclut que $S = \{91k + 31 \mid k \in \mathbb{Z}\}$.

Autrement dit, on a démontré que

$$\begin{cases} n \equiv 3 \quad [7] \\ n \equiv 5 \quad [13] \end{cases} \Leftrightarrow n \equiv 31 \ [91]$$

IV. — P.P.C.M.

1) Définition

Soit a et b deux entiers non nuls et $\mathcal{M}(a, b)$ l'ensemble des multiples positifs communs à a et b. Alors, $|ab| \in \mathcal{M}(a, b)$ donc $\mathcal{M}(a, b)$ est un partie non vide de $\mathbb{N}$ et ainsi $\mathcal{M}(a, b)$ admet un plus petit élément.

Définition 35

Le plus petit élément de $\mathcal{M}(a, b)$ est appelé le plus petit commun multiple de a et b. On le note PPCM(a, b) ou $a \vee b$

Exemple 36.

1. PPCM$(4, 10) = 20$
2. PPCM$(3, 9) = 9$
3. pour tout entier a non nul, PPCM$(1, a) = |a|$.

Remarque 37. Si a et b sont deux entiers non nuls, les multiples positifs communs à a et b sont les mêmes que les multiples positifs communs à $|a|$ et $|b|$ donc $\mathcal{M}(a, b) = \mathcal{M}(|a|, |b|)$ et PPCM(a, b) = PPCM$(|a|, |b|)$. Ainsi, on peut toujours se ramener au cas où a et b sont des entiers naturels.

2) Propriétés

Propriété 38

Soit a et b deux entiers naturels non nuls. On note $d = a \wedge b$ et a' et b' les deux entiers premiers entre eux tels que $a = da'$ et $b = db'$. Alors,

1. $\text{PPCM}(a, b) = da'b'$.

2. tout multiple positif commun à a et b est un multiple positif de $\text{PPCM}(a, b)$.

Démonstration. Notons $\mu = da'b'$ et $m = \text{PPCM}(a, b)$.

Remarquons d'abord que $\mu = a'b = b'a$ donc μ est un multiple positif de a et b et ainsi, par définition, $\mu \geqslant m$.

Considérons un multiple positif M commun à a et b. Alors, il existe des entiers k et ℓ tels que $M = ka = kda'$ et $M = \ell b = \ell db'$. Ainsi, $ka'd = \ell b'd$ et donc, comme $d \neq 0$, $ka' = \ell b'$. Ainsi, b' divise ka'. Or, $a' \wedge b' = 1$ donc, par le théorème de Gauss, b' divise k. Il existe donc un entier h tel que $k = hb'$ et ainsi $M = hb'da' = hda'b'$ donc $M = h\mu$. On a donc montré que μ divise tout multiple positif M commun à a et b.

En particulier, μ divise m donc $\mu \leqslant m$ (car μ et m sont positifs).

Ainsi, on conclut que $m = \mu = da'b'$.

Or, on a montré que tout multiple positif commun à a et b est un multiple de μ donc de m. □

Remarque 39. On a vu précédemment que, pour tous entiers naturels non nuls,

$$c \mid a \text{ et } c \mid b \Leftrightarrow c \mid \text{PGCD}(a, b).$$

Le point **2.** de la propriété précédente permet de voir que, pour tous entiers a, b et c strictement positifs,

$$a \mid c \text{ et } b \mid c \Leftrightarrow \text{PPCM}(a, b) \mid c.$$

Corollaire 40

Soit a, b, c et k des entiers naturels tels que a, b et k soient non nuls. Alors,

1. $\text{PGCD}(a, b)\text{PPCM}(a, b) = ab$. En particulier, si a et b sont premiers entre eux alors $\text{PPCM}(a, b) = ab$.

2. si a et b sont premiers entre eux, si $a \mid c$ et si $b \mid c$ alors $ab \mid c$.

3. $\text{PPCM}(ka, kb) = k\text{PPCM}(a, b)$.

Démonstration. Notons $d = \text{PGCD}(a, b)$, $m = \text{PPCM}(a, b)$ et a' et b' les deux entiers tels que $a = da'$ et $b = db'$.

1. On a montré précédemment que $m = da'b'$ donc $dm = d^2a'b' = (da')(d'b) = ab$.

2. Supposons que a et b sont premiers entre eux et que a et b divise c. Alors, c est un multiple commun à a et b donc c est un multiple de m. Or, a et b sont premiers entre eux donc $m = ab$ et ainsi ab divise c.

3. En appliquant le point **1.** aux entiers ka et kb, il vient

$$\text{PGCD}(ka, kb)\text{PPCM}(ka, kb) = (ka)(kb) = k^2ab.$$

Or, on sait que $\text{PGCD}(ka, kb) = k\text{PGCD}(a, b) = kd$ donc $kd\text{PPCM}(ka, kb) = k^2ab$ i.e., comme $kd \neq 0$,

$$\text{PPCM}(ka, kb) = \frac{k^2ab}{kd} = k\frac{ab}{d} = km$$

d'après le point **1.**

□

Exercice 41.

1. Déterminer PPCM(792, 1638).
2. Soit $n \in \mathbb{N}^*$. On pose $a_n = n^2 + 3n$ et $b_n = (2n+1)(n+3)$. Déterminer PPCM(a_n, b_n).
3. Déterminer les entiers compris entre 7000 et 8000 dont le reste dans la division par 120 et dans la division par 150 est 111.

Solution

1. En utilisant l'algorithme d'Euclide :

$$\begin{aligned} 1638 &= 2 \times 792 + 54 \\ 792 &= 14 \times 54 + 36 \\ 54 &= 36 + \boxed{18} \\ 36 &= 2 \times 18 + 0 \end{aligned}$$

donc $\text{PGCD}(792, 1638) = 18$ et ainsi $\text{PPCM}(792, 1638) = \dfrac{792 \times 1638}{18} = 72072$.

2. Remarquons que

$$\text{PPCM}(a_n, b_n) = \text{PPCM}(n(n+3), (2n+1)(n+3)) = (n+3)\text{PPCM}(n, 2, +1).$$

De plus, $(2n+1) - 2 \times n = 1$ donc, par le théorème de Bézout, $2n+1$ et n sont premiers entre eux donc $\text{PPCM}(2n+1, n) = n(2n+1)$. On conclut donc que $\text{PGCD}(a_n, b_n) = n(2n+1)(n+3)$.

3. Soit N un entier naturel compris entre 7000 et 8000 dont le reste dans le division euclidienne par 120 et par 150 est 111. Alors, 120 et 150 divise $N - 111$ donc $\text{PPCM}(120, 150)$ divise $N - 111$. Or,

$$\text{PPCM}(120, 150) = \text{PPCM}(4 \times 30, 5 \times 30) = 30\text{PPCM}(4, 5) = 30 \times 4 \times 5 = 600$$

car 4 et 5 sont premiers entre eux (puisqu'ils sont consécutifs). Ainsi, 600 divise $N - 111$ donc il existe un entier k tel que $N = 111 + 600k$. De plus, $7000 \leqslant 111 + 600k \leqslant 8000$ donc $\dfrac{6889}{600} \leqslant k \leqslant \dfrac{7889}{600}$ i.e. puisque $k \in \mathbb{Z}$, $k = 12$ ou $k = 13$. On conclut que les seuls entiers possibles sont $111 + 600 \times 12 = 7311$ et $111 + 600 \times 13 = 7911$.

Réciproquement, si $N \in \{7311, 7911\}$ alors 600 divise $N - 111$ donc 120 et 150 divise $N - 111$ donc $N \equiv 111$ [120] et $N \equiv 111$ [150]. Comme $0 \leqslant 111 < 120 < 150$, on conclut que 111 est le reste dans la division euclidienne de N par 120 et 150.

Ainsi, les entiers cherchés sont 7311 et 7911.