Arithmétique

Division euclidienne et PGCD

Définition 1. *Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. On dit que b divise a s'il existe $k \in \mathbb{Z}$ tel que $a = bk$. Dans ce cas, on note $b|a$.*

Exercice 1. Soit $a \in \mathbb{Z}$. On $\mathcal{D}(a)$ l'ensemble des diviseurs de a. Par exemple, $\mathcal{D}(12) = \{-4, -3, -1, 1, 3, 4\}$.

1. Déterminer $\mathcal{D}(15)$.
2. Déterminer $\mathcal{D}(33)$.
3. Déterminer $\mathcal{D}(-8)$.
4. Déterminer $\mathcal{D}(1)$.
5. Déterminer $\mathcal{D}(0)$.
6. Déterminer $\mathcal{D}(15) \cap \mathcal{D}(5)$.
7. Déterminer $\mathcal{D}(-8) \cap \mathcal{D}(0)$.
8. Déterminer $\mathcal{D}(12) \cap \mathcal{D}(18)$.
9. Déterminer $\mathcal{D}(0) \cap \mathcal{D}(n)$, où $n \in \mathbb{Z}$.

Exercice 2. Soient a et b deux entiers. Quel nom donner à $\mathcal{D}(a) \cap \mathcal{D}(b)$?

Exercice 3. Soient, $a, b, c \in \mathbb{Z}$. Prouver les assertions suivantes :

1. $(a|b \text{ et } b|a) \Rightarrow b = \pm a$
2. $(a|b \text{ et } b|c) \Rightarrow a|c$
3. $(a|b \text{ et } a|c) \Rightarrow a|(b + c)$

Exercice 4. Prouver que le produit deux entiers consécutifs est divisible par 2.

Définition 2. *Soit $a, b \in \mathbb{N}$. On appelle* ***plus grand commun diviseur*** *de a et b, le plus grand entier, supérieur ou égal à 1, qui divise à la fois a et b. On le note $pgcd(a, b)$. Autrement dit $pgcd(a, b) = \max \mathcal{D}(a) \cap \mathcal{D}(b)$.*

Exercice 5. Déterminer :

1. pgcd(12,48)
2. pgcd(13,10)
3. pgcd(36,54)
4. pgcd(14,15)
5. pgcd(15,16)
6. pgcd(16,17)

Exercice 6. Prouver que le pgcd de deux entiers consécutifs est 1.

Proposition 1. *Division euclidienne. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}\backslash\{0\}$. Alors, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que*

- $a = bq + r$
- $0 \leq r < b$

Exercice 7. Donner le reste de la division euclidienne de :

1. 23 par 5
2. -12 par 7

3 -49 par 18

Exercice 8. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}\backslash\{0\}$. On note q et r le quotient et le reste de la division euclidienne de a par b.

1. Écrire l'égalité vérifiée par a, b, q et r. Isoler r.
2. Prouver que $\mathcal{D}(a) \bigcap \mathcal{D}(b) \subset \mathcal{D}(b) \bigcap \mathcal{D}(r)$.
3. Dans l'égalité donnée à la question 1., isoler a.
4. Prouver que $\mathcal{D}(b) \bigcap \mathcal{D}(r) \subset \mathcal{D}(a) \bigcap \mathcal{D}(b)$.

Exercice 9. Algorithme d'Euclide. On cherche le pgcd de 498 et 42. On note r_1 le reste de la division euclidienne de 498 par 42.

1. Trouver r_1.

L'exercice précédent permet d'affirmer que $\mathcal{D}(498) \cap \mathcal{D}(42) = \mathcal{D}(42) \cap \mathcal{D}(r_1)$.

2. Est-il plus facile de déterminer $\mathcal{D}(498) \cap \mathcal{D}(42)$ ou $\mathcal{D}(42) \cap \mathcal{D}(r_1)$? Pourquoi ?
3. Déterminer $\mathcal{D}(42) \cap \mathcal{D}(r_1)$. En déduire $\mathcal{D}(498) \cap \mathcal{D}(42)$ puis $pgcd(498, 42)$.

En fait, pour déterminer $\mathcal{D}(42) \cap \mathcal{D}(r_1)$, on aurait pu calculer r_2, le reste de la division euclidienne de 42 par r_1 et constater que $\mathcal{D}(r_1) \cap \mathcal{D}(r_2) = \mathcal{D}(42) \cap \mathcal{D}(r_1) = \mathcal{D}(498) \cap \mathcal{D}(42)$.

4. Déterminer, r_2 puis $\mathcal{D}(r_1) \cap \mathcal{D}(r_2)$ et $pgcd(498, 42)$.

On voit bien que l'on est en train de construire un algorithme pour le pgcd de deux entiers a et b :

-étape 1 : calculer le reste r de la division euclidienne de a par b
-étape 2 :
si $r \neq 0$, remplacer a par b et b par r, et recommencer l'étape 1
si $r = 0$, alors on s'arrête et b est le pgcd des nombres de départ.

5. Continuer l'algorithme pour 498 et 42 jusqu'à ce que le reste de la division euclidienne soit nul.

Exercice 10. Appliquer l'algorithme d'Euclide pour déterminer :

1. pgcd(2555,240)
2. pgcd(292,224)
3. pgcd(1545,585)
4. pgcd(120, 47)

Définition 3. *Soient a et b deux entiers non nuls. On dit que a et b sont **premiers entre eux** si $pgcd(a,b) = 1$.*

Exercice 11. Prouver que 99 et 100 sont premiers entre eux.

Théorème de Bezout

Proposition 2. *Théorème de Bezout.*
Soient a et b des entiers. Il existe des entiers u et v tels que $au + bv = pgcd(a,b)$.

Exercice 12. Soient $a = 92$ et $b = 14$.

1. Ecrire les différentes étapes de l'algorithme d'Euclide pour a et b.
2. A chaque étape, exprimer le reste en fonction du dividende et du diviseur.
3. Exprimer le dernier reste non nul en fonction de a et de b. En déduire u et v tels que $au + bv = \text{pgcd}(a,b)$.

Exercice 13. Soient $a = 226$ et $b = 36$.

1. Ecrire les différentes étapes de l'algorithme d'Euclide pour a et b.
2. A chaque étape, exprimer le reste en fonction du dividende et du diviseur.
3. Exprimer le dernier reste non nul en fonction de a et de b. En déduire u et v tels que $au + bv = \text{pgcd}(a,b)$.

Exercice 14. Soient $a = 736$ et $b = 530$.

1. Calculer $\text{pgcd}(a,b)$.
2. Déterminer deux entiers relatifs n et m tels que $an + bm = \text{pgcd}(a,b)$.

Exercice 15. Considérons l'équation suivante : (E) $78x + 65y = 91$.

1. Montrer que cette équation est équivalente à une équation (E') $ax + by = c$ où $\text{pgcd}(a,b) = 1$.
2. Déterminer une solution particulière (x_0, y_0) de l'équation (E').
3. Résoudre (E) en utilisant le couple (x_0, y_0).
4. Quelle interprétation géométrique donner au problème ?

Exercice 16. Soient a, b et d trois entiers tels que :

- $d|a$
- $d|b$

Démontrer que $d|pgcd(a,b)$.

Exercice 17. Résoudre (dans $\mathbb{Z}^2$) $133x + 368y = 16$.

Exercice 18. Résoudre (dans $\mathbb{Z}^2$) $110x + 235y = 30$.

Exercice 19. Résoudre (dans $\mathbb{Z}^2$) $108x + 225y = 4$.

Exercice 20. Résoudre (dans $\mathbb{Z}^2$) $210x + 126y = 84$.

Exercice 21. Soient a et b deux entiers non nuls. Prouver que :

$$a \text{ et } b \text{ sont premiers entre eux } \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2 : au + bv = 1$$

Exercice 22. Lemme de Gauss. Soient a, b et c trois entiers tels que :

- $a|bc$
- $\text{pgcd}(a,b) = 1$

Démontrer que $a|c$.

Exercice 23. Écrire une fonction python qui prend en paramètres deux entiers et qui retourne leur pgcd.

Exercice 24. Écrire une fonction python qui prend en paramètres deux entiers et qui retourne les coefficients de Bezout associés (u et v tels que $au + bv = pgcd(a,b)$).