Exercice 1 p. 148

1. On a $D(92) = \{1, 2, 4, 23, 46, 92\}$ et $D(64) = \{1, 2, 4, 8, 16, 32, 64\}$.
2. On en déduit que $D(92, 64) = \{1, 2, 4\}$ donc $\text{PGCD}(92, 64) = 4$.

Exercice 3 p. 148

1. L'instruction `mystere(142,76)` renvoie le nombre 2.
2. Cette fonction renvoie le P.G.C.D. des nombres a et b. En effet, partant de $n = 1$ et tant que $n \leqslant a$ et $n \leqslant b$, elle teste si n divise a et b et si c'est le cas, elle stocke n dans la variable p. Ainsi, à la fin de la boucle `while`, p contient le plus grand entier qui divise à la fois a et b i.e. le P.G.C.D. de a et b.

Exercice 6 p. 148. Sachant que le dernier reste non nul dans l'algorithme d'Euclide est le P.G.C.D, les divisions successives sont

$$\begin{aligned} a &= 1 \times b + r_1 \\ b &= 2 \times r_1 + r_2 \\ r_1 &= 1 \times r_2 + r_3 \\ r_2 &= 3 \times r_3 + 504 \\ r_3 &= 2 \times 504 + 0 \end{aligned}$$

Ainsi, $r_3 = 2 \times 504 = 1008$, $r_2 = 3r_3 + 504 = 3528$, $r_1 = r_2 + r_3 = 4536$, $b = 2r_1 + r_2 = 12600$ et $a = b + r_1 = 17136$. On conclut donc que $a = 17136$ et $b = 12600$.

Exercice 9 p. 148. Soit a un entier tel que $600 < a < 1000$ et $\text{PGCD}(a; 630) = 105$. Alors, 105 divise a donc il existe un entier k tel que $a = 105k$ avec $600 < 105k < 1000$ i.e. $\frac{40}{7} < k < \frac{200}{21}$. Comme k est un entier, on en déduit que $k \in \{6; 7; 8; 9\}$ donc $a \in \{630; 735; 840; 945\}$.

Réciproquement, on vérifie (par exemple à la calculatrice) que $\text{PGCD}(630; 630) = 630$, $\text{PGCD}(735; 630) = 105$, $\text{PGCD}(840; 630) = 210$, $\text{PGCD}(945; 630) = 315$ donc, finalement, l'unique solution est $a = 735$.

Exercice 10 p 148

1. Soit $d \in D(a, b)$. Alors, d divise a et b donc d divise toute combinaison linéaire de a et b. En particulier, d divise $A = 3a + 4b$ et $B = 4a + 5b$ donc $d \in D(A, B)$. Ainsi, $D(a, b) \subset D(A, b)$.
2. On remarque que $4B - 5A = 4(4a + 5b) - 5(3a + 4b) = 16a + 20b - 15a - 20b = a$ et que $4A - 3B = 4(3a + 4b) - 3(4a + 5b) = 12a + 16b - 12a - 15b = b$. Ainsi, $a = -5A + 4B$ et $b = 4A - 3B$.
3. Soit $d \in D(A, B)$. Alors, d divise A et B donc d divise toute combinaison linéaire de A et B. En particulier, d divise $a = -5A + 4B$ et $b = 4a - 3B$ donc $d \in D(a, b)$. Ainsi, $D(A, B) \subset D(a, b)$.

   Par le principe de double inclusion, on en déduit que $D(a, b) = D(A, B)$ et donc $\text{PGCD}(a, b) = PGCD(A, B)$.

Remarque. On peut retrouver le résultat de la question **2.** par un calcul matriciel. En effet, le système $\begin{cases} A = 3a + 4b \\ B = 4a + 5b \end{cases}$ a pour écriture matricielle $\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 4 & 5 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$. Le déterminant de la matrice $M = \begin{pmatrix} 3 & 4 \\ 4 & 5 \end{pmatrix}$ est $\det(M) = 3 \times 5 - 4 \times 4 = -1$ donc M est inversible et son inverse est $M^{-1} = \frac{1}{-1} \begin{pmatrix} 5 & -4 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} -5 & 4 \\ 4 & -3 \end{pmatrix}$. Ainsi, $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -5 & 4 \\ 4 & -3 \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} -5A + 4B \\ 4A - 3B \end{pmatrix}$ i.e. $a = -5A + 4B$ et $b = 4A - 3B$.

Le point clé ici est que la matrice M^{-1} est à coefficients entiers et cela vient du fait que $|\det(M)| = 1$. À ce sujet, on pourra consulter le DM 2018 (partie A) du chapitre « Matrices et applications » disponible sur mon site.

Exercice 14 p. 148

1. Comme $\text{PGCD}(n; 18) = 3$, $D(n, 18) = \{1, 3\}$ donc 3 divise n mais 2 ne divise pas n (car il divise 18 donc s'il divisait n, il appartiendrait à $D(n, 18)$). De même, $\text{PGCD}(n; 175) = 5$ donc $D(n; 175) = \{1, 5\}$ et ainsi 5 divise n mais 7 ne divise pas n. Or, $D(42) = \{1, 2, 3, 6, 7, 14, 21, 42\}$ donc, comme n n'est pas divisible par 7, il ne l'est pas non plus par 14, 21 et 42. De plus, comme n est divisible par 3 mais pas par 2, on conclut que $\text{PGCD}(n, 42) = 3$.

   Comme $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$ et comme 2 ne divise pas n, $D(n, 30) \subset \{1, 3, 5, 15\}$. Or, on sait que 1, 3 et 5 sont des diviseurs communs à n et 30 donc $\{1, 3, 5\} \subset D(n, 30)$. Ainsi, $D(n, 30) = \{1, 3, 5\}$ ou $D(n, 30) = \{1, 3, 5, 15\}$. De plus, si on note $d = \text{PGCD}(n, 30)$, on sait que $D(n, 30) = D(d)$ ce qui exclut le premier cas car $\{1, 3, 5\}$ n'est pas l'ensemble des diviseurs de 5. Ainsi, $D(n, 30) = \{1, 3, 5, 15\}$ donc $\text{PGCD}(n, 30) = 15$.

   Remarque. On aimerait dire directement que, puisque n est divisible par 3 et par 5 alors il est divisible par $3 \times 5 = 15$. C'est vrai mais ce n'est pas évident. Par exemple, 12 est divisible par 4 et par 6 mais pas par $4 \times 6 = 24$. On verra plus tard dans quels cas on peut affirmer que si a et b sont deux entiers qui divise un entier n alors ab divise n. Dans tous les cas, le raisonnement précédent montre que $\text{PGCD}(n, 30) = 15$ et donc, en particulier, que 15 divise n.

2. On teste tous les multiples de 15 entre 0 et 100 :

n	0	15	30	45	60	75	90
$\text{PGCD}(n, 18)$	18	3	6	9	6	3	18
$\text{PGCD}(n, 175)$	175	5	5	5	5	75	5

   Ainsi, il n'y a bien qu'une seule solution pour n compris entre 0 et 100, il s'agit de $n = 15$.

Exercice 15 p. 148

1. En testant pour les valeurs de n entre 4 et 13, il semble que le PGCD de a et b soit égal à 1 ou à 5, la valeur 5 étant obtenue seulement lorsque n est de la forme $5k + 3$ avec $k \in \mathbb{N}^*$.

2. **a.** On remarque que $a = 3b + 5$ avec $0 \leqslant 5 < b$ car $n > 3$. Ainsi, la division euclidienne de a par b est $a = 3b + 5$.

   b. Par le lemme d'Euclide, on en déduit que $\text{PGCD}(a, b) = \text{PGCD}(b, 5)$ donc $\text{PGCD}(a, b)$ divise 5. Or, les seuls diviseurs positifs de 5 sont 1 et 5 donc $\text{PGCD}(a, b) \in \{1; 5\}$.

   c. Comme $\text{PGCD}(a, b) = \text{PGCD}(b, 5)$, on a

$$\begin{aligned}\text{PGCD}(a, b) = 5 &\Leftrightarrow \text{PGCD}(b, 5) = 5 \Leftrightarrow 5 \mid b \Leftrightarrow b \equiv 0 \ [5] \\ &\Leftrightarrow n + 2 \equiv 0 \ [5] \Leftrightarrow n \equiv -2 \ [5] \Leftrightarrow n \equiv 3 \ [5].\end{aligned}$$

   Ainsi, on a bien montré que $\text{PGCD}(a, b) = 5$ si et seulement si $n \equiv 3 \ [5]$ ce qui permet de valider la conjecture faite en question 1.

Remarque. On peut vérifier que le résultat reste vrai pour tout entier relatif n mais la preuve précédente ne fonctionne pas car on a besoin du fait que $n > 3$ dans la division euclidienne. Pour le montrer dans le cas général, on peut remarquer que si un entier d divise a et b, il divise $a - 3b = 5$ donc $\text{PGCD}(a, b) \in \{1, 5\}$. Le recours à la division euclidienne entraîne ici une restriction que n'a en fait pas lieu d'être.