Chapitre V

Nombres premiers et arithmétique

Table des matières

Partie A

PGCD, théorème de Bézout et théorème de Gauss

1. Le PGCD de deux nombres entiers

a. Définition

Notation 1.

Soit a, b des entiers relatifs.

— On note $\mathcal{D}_a$ l'ensemble des diviseurs positifs de a i.e.

$$\mathcal{D}_a = \{k \in \mathbb{N} \mid k \text{ divise } a\}.$$

— On note $\mathcal{D}(a, b)$ l'ensemble des diviseurs positifs communs de a et de b i.e.

$$\mathcal{D}(a, b) = \mathcal{D}_a \cap \mathcal{D}_b.$$

Exemple 1.

— $\mathcal{D}_1 = \{1\}$; $\mathcal{D}_2 = \{1, 2\}$; $\mathcal{D}_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$; $\mathcal{D}_{-6} = \{1, 2, 3, 6\}$.

— $\mathcal{D}_0 = \mathbb{N}$ - c'est le seul ensemble de diviseurs infini.

— $\mathcal{D}(4, 6) = \{1, 2\}$; $\mathcal{D}(3, 14) = \{1\}$; $\mathcal{D}(0, a) = \mathcal{D}_a$

Proposition-Notation 1.

Soit a, b des entiers relatifs non tous nuls. L'ensemble $\mathcal{D}(a, b)$ admet un plus grand élément.

Démonstration.

Soit a, b des entiers relatifs non tous nuls. Quitte à échanger a et b, on peut supposer que a est non nul. Alors $\mathcal{D}_a$ est un ensemble majoré par a et donc, comme $\mathcal{D}(a, b) = \mathcal{D}_a \cap \mathcal{D}_b \subset \mathcal{D}_a$, $\mathcal{D}(a, b)$ est majoré par a.
De plus, comme 1 est positif et divise tous les entiers relatifs, 1 appartient à $\mathcal{D}_a$ et $\mathcal{D}_b$ donc $1 \in \mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}(a, b)$.
Par suite, $\mathcal{D}(a, b)$ est une partie non vide et majorée de $\mathbb{N}$, donc elle possède un plus grand élément. □

Définition 1. *PGCD*

Soit a, b des entiers relatifs non tous nuls. On appelle **Plus Grand Commun Diviseur (PGCD) de a et b** et on note $\mathbf{pgcd(a, b)}$ le plus grand élément de l'ensemble $\mathcal{D}(a, b)$ des

diviseurs communs de a et b.

Exemple 2.

$$\text{pgcd}(6,9) = 3 \qquad \text{pgcd}(8,28) = 4 \qquad \text{pgcd}(-10,25) = 5$$
$$\text{pgcd}(21,32) = 1 \qquad \text{pgcd}(0,11) = 11.$$

b. Propriétés

Lemme 1.

Soit a et b des entiers relatifs. Alors on a $\mathcal{D}(a,b) = \mathcal{D}(a-b,b)$ et plus généralement, pour tout $k \in \mathbb{Z}$:

$$\mathcal{D}(a,b) = \mathcal{D}(a-kb,b).$$

Démonstration.

Soit $k \in \mathbb{Z}$. Montrons par double inclusion que $\mathcal{D}(a,b) = \mathcal{D}(a-kb,b)$.

— Montrons que $\mathcal{D}(a,b) \subset \mathcal{D}(a-kb,b)$. Soit $d \in \mathcal{D}(a,b)$.
Alors d divise a et d divise b. Ainsi, par le théorème de combinaison linéaire, d divise $a-kb$ (ici $u=1$ et $v=-k$) et par hypothèse, d divise b. Par suite, d appartient à $\mathcal{D}(a-kb,b)$. Ce qui prouve que $\mathcal{D}(a,b) \subset \mathcal{D}(a-kb,b)$.

— Montrons que $\mathcal{D}(a-kb,b) \subset \mathcal{D}(a,b)$. Soit $d \in \mathcal{D}(a-kb,b)$.
Alors d divise $a-kb$ et d divise b. Ainsi, par le théorème de combinaison linéaire, d divise $a = (a-kb)+kb$ (ici $u=1$ et $v=k$) et par hypothèse, d divise b. Par suite, d appartient à $\mathcal{D}(a,b)$. Ce qui prouve que $\mathcal{D}(a-kb,b) \subset \mathcal{D}(a,b)$.

Par double inclusion, il en résulte que $\mathcal{D}(a,b) = \mathcal{D}(a-kb,b)$. □

Proposition 2. *Propriétés du PGCD*

Soit a et b des entiers relatifs non tous nuls.

i) Pour tout $k \in \mathbb{Z}$, $\text{pgcd}(a,b) = \text{pgcd}(a-b,b) = \text{pgcd}(a-kb,b)$.

ii) Si $0 < b < a$ et r est le reste de la division euclidienne de a par b :

$$\text{pgcd}(a,b) = \text{pgcd}(r,b)$$

iii) Si $b > 0$ et b divise a, $\text{pgcd}(a,b) = b$.

Démonstration.

i) Soit $k \in \mathbb{Z}$. D'après le lemme précédent, on a $\mathcal{D}(a,b) = \mathcal{D}(a-kb,b)$. Or comme a, b sont non tous nuls et donc également $a-kb$ et b, ces deux paires de nombres possèdent un pgcd. Par définition, leurs pgcds respectifs sont les plus grands éléments de $\mathcal{D}(a,b)$ et de

$\mathcal{D}(a-kb,b)$. Comme ces ensembles sont égaux, leurs plus grands éléments respectifs sont égaux d'où $\text{pgcd}(a,b) = \text{pgcd}(a-kb,b)$

ii) On effectue la division eulidienne de a par b. Alors il existe un couple d'entiers (q,r) tel que $a = bq + r$ avec $0 \leq r < b$. On a alors $r = a - bq$ et donc, d'après le point précédent, comme $q \in \mathbb{Z}$:

$$\text{pgcd}(a,b) = \text{pgcd}(a-qb,b) = \text{pgcd}(r,b)$$

iii) Si b divise a, alors, le reste r de la division euclienne de a par b est nul, donc, d'après le point précédent :

$$\text{pgcd}(a,b) = \text{pgcd}(0,b) = b.$$

□

c. Algorithme d'Euclide

La propriété *ii)* de la proposition 2 nous permet d'obtenir un algorithme pratique du calcul du PGCD de deux entiers :

Algorithme d'Euclide

```
def euclide(a,b):
    """ renvoie le pgcd de a et b entiers relatifs grâce à l'algorithme d'Euclide """
    r=b
    while r !=0:
        r=a%b #reste de la division euclienne de a par b
        a=b
        b=r
    return a
```

Exercice 1.

Soit a, b deux entiers naturels non nuls tel que $0 < b < a$ et b ne divise pas a.
Soit $(r_n)_{n\in\mathbb{N}}$ la suite des valeurs de la variable r dans l'algorithme d'Euclide.

1. En utilisant une deuxième suite d'entiers relatifs $(q_n)_{n\in\mathbb{N}}$, déterminer une relation de récurrence entre r_{n+1} et r_n.
2. Montrer qu'il existe $N \in \mathbb{N}$ tel que $r_N \neq 0$ et et pour tout $n > N$, $r_n = 0$.
3. Montrer que $r_N = \text{pgcd}(a,b)$.

Proposition 3.

Soit a, b deux entiers relatifs non nuls tel que $0 < b < a$ et b ne divise pas a.
Si r est le dernier reste non nul de l'algorithme d'Euclide, alors

$$\text{pgcd}(a,b) = r.$$

De plus, les diviseurs communs de a et b sont exactement les diviseurs de $\text{pgcd}(a,b)$ i.e.

$$\mathcal{D}(a,b) = \mathcal{D}_{\text{pgcd}(a,b)}.$$

Exercice 2.

Calculer le PGCD de 456 et 24 ; de 565 et 121 et de 121 et 18.

Proposition 4.

Soit a, b des entiers relatifs non nuls et c un entier naturel. On a :

$$\text{pgcd}(ac, bc) = c \times \text{pgcd}(a, b).$$

d. Nombres premiers entre eux

Définition 2.

Soit a et b deux entiers relatifs non tous nuls. On dit que a et b sont **premiers entre eux** si $\text{pgcd}(a, b) = 1$; sinon, ils ne le sont pas.

Proposition 5.

Soit a et b deux entiers relatifs non tous nuls. Si a et b sont premiers entre eux, alors 1 est le seul diviseur positif commun à a et b.

Méthode pour montrer que deux entiers a et b sont premiers entre eux :
On applique l'algorithme d'Euclide à a et b : si le dernier reste non nul est 1, a et b sont premiers entre eux.

Exercice 3.

1. Montrer que 2173 et 1961 ne sont pas premiers entre eux alors que 2173 et 1962 le sont.
2. Exercices 1 à 10 p148

Théorème 1.

Soit a, b des entiers relatifs non nuls et d un entier naturel non nul. Alors on a : $d = \text{pgcd}(a, b)$ si, et seulement si, il existe a', b' des entiers relatifs tels que :

$$a = da',\ b = db' \text{ ET } a' \text{ et } b' \text{ sont premiers entre eux.}$$

e. Exercices

Exercice 4.

Soit n un entier naturel. Déterminer $\text{pgcd}(n+3, 2n+1)$ en fonction de n.

Correction.

On pose $d = \text{pgcd}(n+3, 2n+1)$. Alors d divise $n+3$ et $2n+1$ donc d divise la combinaison linéaire $2(n+3) - (2n=1) = 5$. Ainsi $d = 1$ ou $d = 5$.
On remarque alors que $d = 5$ si, et seulement si, 5 divise $n+3$ et $2n+1$ i.e.

$$n+3 \equiv 0 \bmod 5 \ (1) \quad \text{et} \quad 2n+1 \equiv 0 \bmod 5 \ (2)$$

si on calcule $(2) - (1)$, on obtient alors :

$$n \equiv 2 \bmod 5$$

i.e. $n = 5k+2$ pour $k \in \mathbb{N}$.
Réciproquement, on remarque que si $n = 5k+2$ pour $k \in \mathbb{N}$, alors 5 divise $n+3$ et 5 divise $2n+1$ et donc $d = 5$.
Il en résulte que pour $n = 5k+2$ avec $k \in \mathbb{N}$,

$$\text{pgcd}(n+3, 2n+1) = 5$$

et das les autres cas :

$$\text{pgcd}(n+3, 2n+1) = 1$$

Exercice résolu 3 p139 ; exercice 14,15 p148

Exercice 5.

Déterminer tous les couples d'entiers (a, b) avec $0 < a < b$ tels que

$$\begin{cases} ab = 3468 \\ \text{pgcd}(a, b) = 17 \end{cases}$$

Correction.

$\text{pgcd}(a, b) = 17$ est équivalent à $a = 17a'$ et $b = 17b'$ où a' et b' sont des entiers premiers entre eux.
Par suite, on a :

$$3468 = ab = 17^2 a'b'$$

Or $3468 = 17^2 \times 6$ donc $a'b' = 12$ d'où, comme $a' < b'$, les couples possibles pour (a', b') sont :

$$(1, 12), \ (2, 6), \ \text{et} \ (3, 4)$$

De plus, comme $\text{pgcd}(a', b') = 1$, le couple $(2, 6)$ ne convient pas.

Il en résulte que les seuls couples $(a, b) = (17a', 17b')$ vérifiant le problème sont :

$$(17, 17 \times 12) = (17, 204) \text{ et } (17 \times 3, 17 \times 4) = (51, 68).$$

Exercice résolu 3 p141 ; exercice 47,48 p151 (pour le 48, le faire tel quel puis le refaire en remplaçant 9792 par 9728).

2. Théorème de Bézout et théorème de Gauss

a. Théorème de Bézout

Proposition 6. *Relation de Bézout*

Soit a, b des entiers non tous nuls et $d = \text{pgcd}(a, b)$. Alors il existe u, v des entiers **relatifs** tels que :

$$au + bv = d$$

Démonstration.

On remonte l'algorithme d'Euclide ! □

Méthode : pour trouver une combinaison linéaire de a et b égale au PGCD de a et b, on remonte l'algorithme d'Euclide

Exercice 6.

Déterminer une relation de Bézout pour le couple $(45, 81)$

Correction.

L'algorithme d'Euclide nous donne :

$$\begin{array}{rcrcrcrcrcr} 81 & = & 1 \times 45 & + & 36 & \rightarrow & 36 & = & 81 & - & 1 \times 45 \\ 45 & = & 1 \times 36 & + & 9 & \rightarrow & 9 & = & 45 & - & 1 \times 36 \\ 36 & = & 4 \times 9 & + & 0 & & & & & & \end{array}$$

Donc on a $\text{pgcd}(81, 45)$. Maintenant, on remonte l'algorithme d'Euclide en utilisant les expressions écrites en vert, en partant de la ligne du PGCD (*Attention, bien faire étape par étape en développant les parenthèses après chaque substitution*).

$$\begin{aligned} 9 &= 45 - 1 \times 36 \\ 9 &= 45 - 1 \times (81 - 1 \times 45) \\ 9 &= 2 \times 45 - 1 \times 81 \\ 9 &= 81 \times (-1) + 45 \times 2 \end{aligned}$$

Ainsi, on a trouvé la relation de Bézout $81u + 45v = \text{pgcd}(81, 45) = 9$ avec $u = -1$ et $v = 2$.

Remarque : il n'y a pas qu'une seule relation de Bézout : en fait, comme on le verra dans la suite du cours, il existe une infinité de couple (u, v) qui conviennent !

Voire exercice résolu 1 p141

Théorème 2. *Théorème de Bézout*

Soit a, b des entiers non nuls.
Les entiers a et b sont premiers entre eux **si, et seulement si,** il existe u, v des entiers **relatifs** tels que

$$au + bv = 1$$

Démonstration.

Il s'agit d'une équivalence, on démontre donc les deux implications :

($\Rightarrow$) On suppose que a et b sont premiers entre eux. Montrons qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Comme a, b sont premiers entre eux, alors, par définition, leur PGCD est égal à 1. Ainsi, d'après la relation de Bézout (Proposition 6), il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

($\Leftarrow$) On suppose qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Montrons que a, b sont premiers entre eux.

On note $d = \text{pgcd}(a, b)$. Alors en particulier, d divise a et d divise b. Ainsi, par combinaison linéaire, d divise $au + bv = 1$ et donc d divise 1. Or un PGCD est un entier supérieur ou égal à 1, donc $d = 1$.
Il en résulte que a et b sont premiers entre eux.

□

Exercice 7.

1. Soit $n \in \mathbb{N}$. Montrer que $7n + 4$ et $5n + 3$ sont premiers entre eux.
2. Soit a, b, c des entiers naturels non nuls. Montrer que si a est premier avec b et a est premier avec c alors a est premier avec bc.

Démonstration.

1. Soit $n \in \mathbb{N}$. On a $(5n+3) \times 7 + (7n+4) \times (-5) = 1$ donc on a trouvé une combonaison linéaire de la forme $(5n+3)u + (7n+4)v = 1$ où u, v sont des entiers relatifs donc d'après le théorème de Bézout (l'implication $\Leftarrow$), $5n+3$ et $7n+4$ sont premiers entre eux.

2. Soit $a, b, c \in \mathbb{N}^*$. On suppose que a, b sont premiers entre eux et a, c sont premiers entre eux. Montrons que a et bc sont premiers entre eux.
   D'après le théorème de Bézout (l'implication $\Rightarrow$), il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$ et il existe $u', v' \in \mathbb{Z}$ tels que $au' + cv' = 1$.
   D'où on a $(au+bv)(au'+cv') = 1 \times 1 = 1$; or

$$(au+bv)(au'+cv') = auau' + aucv' + bvau' + bvcv' = a\underbrace{(uau' + ucv' + bvu')}_{=u'' \in \mathbb{Z}} + bc\underbrace{(vv')}_{=v'' \in \mathbb{Z}}.$$

   Ainsi, on a trouvé $u'', v'' \in \mathbb{Z}$ tels que $au'' + (bc)v'' = 1$. Il en résulte, d'après le théorème de Bézout (l'implication $\Leftarrow$), que a et bc sont premiers entre eux.

□

Voire exercice 17 à 20 p149

Méthode : Trouver une solution d'une équation du type $\mathbf{ax + by = n}$ d'inconnues entières x, y et où $a, b, n \in \mathbb{Z}$ (a, b non tous nuls).

- On calcule $d = \text{pgcd}(a, b)$ (avec l'algorithme d'Euclide) ;
- Si d **ne** divise **pas** n, il n'y a aucune solution.
- Si d **divise** n, il existe au moins une solution (il en existe en fait une infinité, on verra cela dans la suite). Voilà comment en déterminer une :
  - on remonte l'algorithme d'Euclide pour déterminer $u, v \in \mathbb{Z}$ tels que $au + bv = d$;
  - comme d divise n, il existe $k \in \mathbb{Z}$ (à determiner concrètement) tel que $n = dk$;
  - ainsi, on a :
$$a(uk) + b(vk) = dk = n.$$
    Donc le couple d'entiers (x_0, y_0) où $x_0 = uk$ et $y_0 = vk$ est solution de $ax + by = n$.

Exercice 8.

Déterminer un couple d'entiers relatifs (x, y) tels que :

1. $59x + 27y = 1$
2. $59x + 27y = 10$
3. $12x + 18y = 30$
4. $12x + 18y = 21$

Correction.

1. On détermine le PGCD de 59 et 27 avec l'algorithme d'Euclide :
$$\begin{array}{rcrcrcrcrcr} 59 & = & 2\times 27 & + & 5 & \to & 5 & = & 59 & - & 2\times 27 \\ 27 & = & 5\times 5 & + & 2 & \to & 2 & = & 27 & - & 5\times 5 \\ 5 & = & 2\times 2 & + & 1 & \to & 1 & = & 5 & - & 2\times 2 \\ 2 & = & 2\times 1 & + & 0 & & & & & & \end{array}$$
On a $\text{pgcd}(59,27) = 1$ divise 1 donc il existe au moins un couple solution. On remonte l'algorithme *(on remplace un reste à chaque étape et on développe la parenthèse avant de refaire une substitution !)* :
$$\begin{array}{rcl} 1 & = & 5-2\times 2 \\ 1 & = & 5-2\times(27-5\times 5) \\ 1 & = & 11\times 5-2\times 27 \\ 1 & = & 11\times(59-2\times 27)-2\times 27 \\ 1 & = & 11\times 59-24\times 27 \\ 1 & = & 59\times 11+27\times(-24) \end{array}$$
Donc le couple $(11,-24)$ est solution !
2. On a $\text{pgcd}(59,27) = 1$ (voir question précédente) divise 10 (et $10 = 10\times 1$) donc il existe au moins une solution. De plus, on a $59\times 11+27\times(-24) = 1$ donc :
$$10 = 10\times 1 = 10\times(59\times 11+27\times(-24)) = 59\times 110+27\times(-240).$$
Ainsi $(110,-240)$ est un couple solution de $59x+27y = 10$.

Voire exercice résolu 1 p143 et exercices 22 p149 ; 33-34p150

b. Théorème de Gauss

Théorème 3. *Théorème de Gauss*

Soit a,b,c des entiers *naturels* non nuls. Si a est *premier avec* b et a divise bc alors a divise c.

Corollaire 1.

Soit n,a,b des entiers naturels non nuls. Si a divise n, b divise n et a,b sont premiers entre eux alors ab divise n.

Exercice 9.

Déterminer tous les couples d'entiers relatifs (x,y) tels que :
1. $59x+27y = 1$
2. $59x+27y = 10$
3. $12x+18y = 30$

4. $12x + 18y = 21$

Voire exercice résolu 2 p143 et exercices 36p150

3. Résolution d'équations

a. Inversibles modulo n

Définition 3.

Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On dit que a est **inversible** modulo n s'il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \mod n$.

Proposition 7.

Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. L'entier a est inversible modulo n si, et seulement si, a et n sont premiers entre eux.

Exercice 10.

Déterminer, si elle existe, une inverse de : 4 modulo 5 ; 2 modulo 9 ; 3 modulo 6, 52 modulo 163.

Correction.

— 4 et 5 sont premiers entre eux donc 4 possède une inverse modulo 5. Comme 5 est "petit", on peut rechercher l'inverse de 4 parmi les restes possibles modulo 5 i.e. 0, 1, 2, 3 et 4.
On remarque que $4 \times 4 = 16 \equiv 1\ [5]$ donc 4 est une inverse de 4 modulo 5.
On pouvait également remarquer que $4 \equiv -1\ [5]$ donc $4 \times 4 \equiv (-1) \times (-1) = 1\ [5]$.
En fait, plus généralement, $n-1$ est sa propre inverse modulo n car $n-1 \equiv -1\ [n]$ donc $(n-1) \times (n-1) \equiv (-1) \times (-1) = 1\ [n]$.

— 2 et 9 sont premiers entre eux donc 2 possède une inverse modulo 9. Comme 9 est "petit", on peut rechercher l'inverse de 2 parmi les restes possibles modulo 9 i.e. de 0 jusqu'à 8.
On remarque que $2 \times 5 = 10 \equiv 1\ [9]$ donc 5 est une inverse de 2 modulo 9.

— 3 et 6 ne sont premiers pas entre eux donc 3 ne possède pas d'inverse modulo 6.

— Comme 163 est "grand", le technique précédente serait trop longue : on calcule donc le pgcd de 52 et 163 via l'algorithme d'Euclide.

$$\begin{array}{rcrcrcrcrcr} 163 & = & 52 \times 3 & + & 7 & \rightarrow & 7 & = & 163 & - & 52 \times 3 \\ 52 & = & 7 \times 7 & + & 3 & \rightarrow & 3 & = & 52 & - & 7 \times 7 \\ 7 & = & 3 \times 2 & + & 1 & \rightarrow & 1 & = & 7 & - & 3 \times 2 \\ 3 & = & 1 \times 3 & + & 0 & & & & & & \end{array}$$

On a donc $\text{pgcd}(52, 163) = 1$ divise 1 donc 52 possède une inverse modulo 163.
On remonte l'algorithme pour trouver une inverse :

$$\begin{aligned} 1 &= 7 - 3 \times 2 \\ 1 &= 7 - (52 - 7 \times 7) \times 2 \\ 1 &= 7 \times 15 - 52 \times 2 \\ 1 &= (163 - 52 \times 3) \times 15 - 52 \times 2 \\ 1 &= 163 \times 15 - 52 \times 47 \\ 1 &= 163 \times 15 + 52 \times (-47) \end{aligned}$$

Ainsi $1 = 163 \times 15 + 52 \times (-47) \equiv 52 \times (-47) \mod 163$, et donc -47 est une inverse de 52 modulo 163.
On peut remarquer que $116 = -47 + 163 \equiv (-47) \mod 163$ donc $52 \times 116 \equiv 52 \times (-47) \equiv 1 \mod 163$. Par suite, 116 est également une inverse de 52 modulo 163.

Exercice 11.

Résoudre les équations suivantes où l'inconnue x est un entier relatif :

$$3x \equiv 1 \mod 5 \qquad 6x + 2 \equiv 0 \mod 17 \qquad 4 - 52x \equiv 14 \mod 163$$

Correction.

Pour ce type d'exercice, on cherche à mettre l'équation initiale $ax \equiv b \mod n$ sous la forme $x \equiv ? \mod n$ en multipliant l'équation par une inverse de a modulo n (si elle existe bien-sûr !). Ainsi on conclut que les solutions sont les $? + nk$ pour $k \in \mathbb{Z}$.

— On remarque que 2 est une inverse de 3 modulo 5 donc :

$$\begin{aligned} & 3x \equiv 1 \mod 5 \\ \Leftrightarrow \quad & \underbrace{(2 \times 3)}_{\equiv 1\ [5]} x \equiv 2 \times 1 \mod 5 \\ \Leftrightarrow \quad & x \equiv 2 \mod 5 \end{aligned}$$

Par suite, l'ensemble des solutions est $\{2 + 5k \mid k \in \mathbb{Z}\}$.

— On met tout d'abord l'équation sous le forme $ax \equiv b \mod n$:

$$\begin{aligned} & 6x + 2 \equiv 0 \mod 17 \\ \Leftrightarrow \quad & 6x \equiv -2 \mod 17 \end{aligned}$$

On remarque que 3 est une inverse de 6 modulo 17 (de "tête" ou en utilisant l'algorithme d'Euclide) donc :

$$\begin{aligned} & 6x \equiv -2 \mod 17 \\ \Leftrightarrow \quad & \underbrace{(3 \times 6)}_{\equiv 1\ [17]} x \equiv 3 \times (-2) \mod 17 \\ \Leftrightarrow \quad & x \equiv -6 \mod 17 \end{aligned}$$

Par suite, l'ensemble des solutions est $\{-6 + 17k \mid k \in \mathbb{Z}\}$.

— On met tout d'abord l'équation sous le forme $ax \equiv b \mod n$:

$$\begin{aligned} & 4 - 52x \equiv 14 \mod 163 \\ \Leftrightarrow \\ & -10 \equiv 52x \mod 163 \end{aligned}$$

On a vu que -47 est une inverse de 52 modulo 163 donc :

$$\begin{aligned} & 52x \equiv -10 \mod 163 \\ \Leftrightarrow \\ & \underbrace{((-47) \times 52)}_{\equiv 1\ [163]} x \equiv (-47) \times (-10) \mod 163 \\ \Leftrightarrow \\ & x \equiv 470 \equiv 144 \mod 163 \end{aligned}$$

Par suite, l'ensemble des solutions est $\{144 + 163k \mid k \in \mathbb{Z}\}$.