# Arithmétique partie II PGCD

D Soit $E$ un sous-ensemble, on dit aussi une partie, de $\mathbb{Z}$
• $m \in \mathbb{Z}$ est **un majorant** de $E$ lorsque $m$ est supérieur ou égal à tout élément de $E$ : $\forall x \in E, x \leqslant m$
• la partie $E$ **est majorée**, on dit aussi l'ensemble $E$ **est majoré**, s'il existe $m \in \mathbb{Z}$ tel que $m$ est majorant de $E$ : $\exists m \in \mathbb{Z}, \forall x \in E, x \leqslant m$
• $m \in \mathbb{Z}$ est le **plus grand élément de** $E$ lorsque $m$ est un majorant de $E$ et $m$ appartient à $E$, on dit alors que $m$ est le maximum de $E$ : $m \in E$ et $\forall x \in E, x \leqslant m$, le maximum de $E$ se note $\max E$

P (Admise) Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.

D **Quelques définitions**
• deux entiers relatifs sont non simultanément nuls lorsque l'un au moins est différent de zéro
• si $a$ et $b$ sont deux entiers relatifs non simultanément nuls alors l'ensemble des diviseurs communs à $a$ et $b$ est une partie non vide et majorée de $\mathbb{Z}$ donc elle admet un plus grand élément noté $\mathrm{PGCD}(a,b)$ ou $\mathrm{PGCD}(a;b)$

P Soient $a$ et $b$ deux entiers relatifs non simultanément nuls, on a immédiatement :

▶ $\boldsymbol{\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,a)}$.

**A01** Donner la liste des diviseurs de $(-10)$ et celle des diviseurs de $15$, en déduire la liste des diviseurs communs puis $\mathrm{PGCD}(-10,15)$.

**A02** Donner la liste des diviseurs de $7$ et celle des diviseurs de $0$, en déduire la liste des diviseurs communs puis $\mathrm{PGCD}(7,0)$.

**A03** Peut-on définir le $\mathrm{PGCD}(a,b)$ lorsque $a$ et $b$ sont tous deux nuls ?

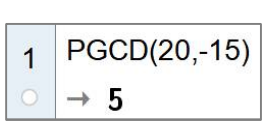
P Soient $a$ et $b$ deux entiers relatifs non simultanément nuls, on a :

▶ $\boldsymbol{\mathrm{PGCD}(a,b) = \mathrm{PGCD}(a,-b) = \mathrm{PGCD}(-a,b) = \mathrm{PGCD}(-a,-b)}$

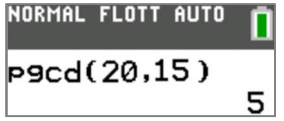
▶ $\boldsymbol{\mathrm{PGCD}(a,b) = \mathrm{PGCD}(|a|,|b|)}$

i Les listes des diviseurs communs de $a$ et $b$, et celle des diviseurs positifs en communs de $a$ et $b$ sont différentes mais **ont le même plus grand élément** : dans la recherche du PGCD on pourra donc ne s'intéresser qu'aux listes des diviseurs **positifs**.

i Utilisation d'outils informatiques




```
>>> from math import *
>>> gcd(20,-15)
5
```




TI83 exige des entiers tous deux strictement **positifs**

F ▶si $a \in \mathbb{Z} \setminus \{0\}$ :
$\mathrm{PGCD}(a,0) = \mathrm{PGCD}(0,a) = |a|$ et $\mathrm{PGCD}(a,a) = |a| \quad (a \neq 0)$

▶si $\boldsymbol{a \in \mathbb{N} \setminus \{0\}}$ :
$\boldsymbol{\mathrm{PGCD}(a,0) = \mathrm{PGCD}(0,a) = a}$ et $\boldsymbol{\mathrm{PGCD}(a,a) = a \quad (a > 0)}$

**A04** Justifier les deux formules précédentes.

**A05** $\mathrm{PGCD}(5,0), \mathrm{PGCD}(0,-3), \mathrm{PGCD}(7,7), \mathrm{PGCD}(-4,-4) = ?$

F Pour $a \in \mathbb{Z}$, on a :
▶ $\boldsymbol{\mathrm{PGCD}(a,1) = \mathrm{PGCD}(1,a) = 1}$

**A06** Justifier la formule précédente.

**A07** $\mathrm{PGCD}(1,7), \mathrm{PGCD}(0,1), \mathrm{PGCD}(-5,1), \mathrm{PGCD}(1,1) = ?$

P Soient $a$ et $b$ deux entiers relatifs non simultanément nuls, on a :
▶ $\boldsymbol{\mathrm{PGCD}(a,b) \geqslant 1}$

$D$ Soit $E$ un sous-ensemble (une partie) de $\mathbb{Z}$

• $m \in \mathbb{Z}$ est **un majorant** de $E$ lorsque $m$ est supérieur ou égal à tout élément de $E$

• la partie $E$ **est majorée** (l'ensemble $E$ **est majoré**) s'il existe $m \in \mathbb{Z}$ tel que $m$ est majorant de $E$

• $m \in \mathbb{Z}$ est le **plus grand élément de** $E$ lorsque $m$ est un majorant de $E$ et $m$ appartient à $E$, on dit alors que $m$ est le maximum de $E$ et on écrit $m = \max E$ ou $m = \max\{\dots\}$

$P$ (Admise) Toute partie **non vide et majorée** de $\mathbb{Z}$ **admet un plus grand élément**.

$D$ **Quelques définitions**

• on dit de que deux entiers relatifs qu'ils sont non simultanément nuls lorsque l'un au moins est différent de zéro

• si $a$ et $b$ sont deux entiers relatifs non simultanément nuls alors l'ensemble des diviseurs communs à $a$ et $b$ est une partie non vide et majorée de $\mathbb{Z}$ donc elle admet un plus grand élément appelé PGCD de $a$ et $b$ et qui se note $\mathrm{PGCD}(a,b)$ ou $\mathrm{PGCD}(a;b)$

$P$ Soient a et b deux entiers relatifs non simultanément nuls, on a immédiatement : $\mathbf{PGCD}(a,b) = \mathbf{PGCD}(b,a)$.

**A01 Donner la liste des diviseurs de $-10$, des diviseurs de $15$, en déduire la liste des diviseurs communs puis $\mathbf{PGCD}(-10,15)$.**

diviseurs de $-10$ : $-10,\ -5,\ -2,\ -1,\ 1,\ 2\ ,\ 5,\ 10.$
diviseurs de $15$ : $-15,\ -5,\ -3, -1,\ 1,\ 3,\ 5,\ 15.$
diviseurs en commun : $-5, -1, 1, 5.$
Le plus grand nombre de la liste des diviseurs communs est $5$ donc $\mathbf{PGCD}(-10,15) = 5$.

**A02 Donner la liste des diviseurs de $7$ et celle des diviseurs de $0$, en déduire la liste des diviseurs communs puis $\mathbf{PGCD}(7,0)$.**

diviseurs de $7$ : $-7,\ -1, 1,\ 7$
diviseurs de $0$ : tout entier relatif
diviseurs en commun : $-7, -1, 1, 7$
Le plus grand nombre de la liste des diviseurs communs est $7$ donc $\mathbf{PGCD}(7,0) = 7$.

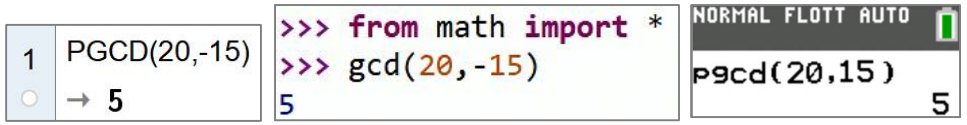
**A03 Peut-on définir le $\mathbf{PGCD}(a,b)$ lorsque $a$ et $b$ sont tous deux nuls ?**

diviseurs de $a = 0$ : tout entier relatif
diviseurs de $b = 0$ : tout entier relatif
diviseurs en commun : tout entier relatif
Il n'y a pas de plus grand nombre dans la liste des diviseurs en commun : **dans le cas de deux entiers nuls le PGCD n'existe pas**.

$P$ Si $a$ et $b$ sont deux entiers relatifs non simultanément nuls alors :
• $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(a,-b) = \mathrm{PGCD}(-a,b) = \mathrm{PGCD}(-a,-b)$
• $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(|a|,|b|)$

$i$ Les listes des diviseurs communs de $a$ et $b$, et celle des diviseurs positifs en communs de $a$ et $b$ sont différentes mais **ont le même plus grand élément** : dans la recherche du PGCD on pourra donc ne s'intéresser qu'aux listes des diviseurs **positifs**.

$i$ Utilisation d'outils informatiques




TI83 exige des entiers strictement **positifs**.

$F$ ▶si $a \in \mathbb{Z} \setminus \{0\}$ :
$\mathrm{PGCD}(a,0) = \mathrm{PGCD}(0,a) = |a|$ et $\mathrm{PGCD}(a,a) = |a|\ \ (a \neq 0)$

▶si $\boldsymbol{a} \in \mathbb{N} \setminus \{\mathbf{0}\}$ :
$\mathbf{PGCD}(a,0) = \mathbf{PGCD}(0,a) = a$ et $\mathbf{PGCD}(a,a) = a\ \ (a > 0)$

**A04 Justifier les formules précédentes.**

• $\boldsymbol{a \in \mathbb{Z} \setminus \{0\}}$

$-$ **montrons que : $\mathbf{PGCD}(a, 0) = \mathbf{PGCD}(0, a) = |a|$**

diviseurs positifs de $a$ : commence par 1 et se termine par $|a|$

diviseurs positifs de 0 : tout entier naturel

plus grand diviseur positif commun : $|a|$ donc : $\mathrm{PGCD}(a, 0) = |a|$

Comme $\mathrm{PGCD}(0, a) = \mathrm{PGCD}(a, 0)$ on en déduit :

$\mathbf{PGCD}(a, 0) = \mathbf{PGCD}(0, a) = |a|$

$-$ **montrons que : $\mathbf{PGCD}(a, a) = |a|$**

diviseurs positifs de $a$ : commence par 1 et se termine par $|a|$

diviseurs positifs de $a$ : commence par 1 et se termine par $|a|$

plus grand diviseur commun positif : $|a|$ donc : $\mathrm{PGCD}(a, 0) = |a|$

• $\boldsymbol{a \in \mathbb{N} - \{0\}}$

Comme $a > 0$, on a $|a| = a$ donc les formules précédentes deviennent : $\mathrm{PGCD}(a, 0) = \mathrm{PGCD}(0, a) = a$ et $\mathrm{PGCD}(a, 0) = a$

**A05 Déterminer :**

**$\mathbf{PGCD}(5, 0)$, $\mathbf{PGCD}(0, -3)$, $\mathbf{PGCD}(7, 7)$, $\mathbf{PGCD}(-4, -4)$.**

On a : $\mathrm{PGCD}(5,0) = 5$, $\mathrm{PGCD}(0, -3) = |-3| = 3$, $\mathrm{PGCD}(7,7) = 7$ et $\mathrm{PGCD}(-4, -4) = |-4| = 4$.

F Pour $a \in \mathbb{Z}$, on a : $\mathrm{PGCD}(a, 1) = \mathrm{PGCD}(1, a) = 1$.

**A06 Justifier la formule précédente.**

diviseurs positifs de 1 : 1

diviseurs positifs de $a$ : commence par 1 et fini par $|a|$

plus grand diviseur positif commun : 1

donc $\mathrm{PGCD}(1, a) = |a|$.

Comme $\mathrm{PGCD}(a, 1) = \mathrm{PGCD}(a, 1)$ on en déduit :

$\mathrm{PGCD}(\mathrm{a}, 1) = \mathrm{PGCD}(1, \mathrm{a}) = 1$.

**A07 $\mathbf{PGCD}(1, 7)$, $\mathbf{PGCD}(0, 1)$, $\mathbf{PGCD}(-5, 1)$ et $\mathbf{PGCD}(1, 1)$.**

$\mathrm{PGCD}(1,7) = 1$, $\mathrm{PGCD}(0,1) = 1$, $\mathrm{PGCD}(-5,1) = 1$, $\mathrm{PGCD}(1,1) = 1$

P Soient $a$ et $b$ deux entiers relatifs non simultanément nuls, on a :

▶ $\mathbf{PGCD}(a, b) \geqslant 1$

**[P] Théorème « PGCD et divisibilité »**

$a \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{Z}$, on a l'équivalence : ▶ $a|b \Leftrightarrow \text{PGCD}(a,b) = |a|$.

$a \in \mathbb{N} \setminus \{0\}$, $b \in \mathbb{Z}$, on a l'équivalence : ▶ $\boldsymbol{a|b \Leftrightarrow \text{PGCD}(a,b) = a}$

**A08** On se propose de démontrer le théorème «PGCD et divisibilité».
On rappelle que, pour deux nombres $x$ et $y$ on a l'équivalence :
$x = y \Leftrightarrow x \leqslant y$ et $y \leqslant x$. Soient $a$ et $b$ deux entiers relatifs, $a \neq 0$.

1. **Démontrons que : $\boldsymbol{a|b \Rightarrow \text{PGCD}(a,b) = |a|}$.**
   On suppose que $a|b$.
   - **a.** Montrer que $|a|$ est un diviseur commun de $a$ et $b$.
     En déduire que : $|a| \leqslant \text{PGCD}(a,b)$.
   - **b.** En utilisant le fait que $\text{PGCD}(a,b)$ est un diviseur de $a \neq 0$, justifier que $\text{PGCD}(a,b) \leqslant |a|$.
   - **c.** Conclure.
2. **Démontrons que : $\boldsymbol{\text{PGCD}(a,b) = |a| \Rightarrow a|b}$.**
   On suppose que : $\text{PGCD}(a,b) = |a|$.
   Montrer que $|a|$ divise $b$, en déduire $a|b$ puis conclure.

*On vient de montrer que, pour $a \neq 0$ : $a|b \Leftrightarrow \text{PGCD}(a,b) = |a|$.*

**[F] Formule de la soustraction**

Pour $a$ et $b$ entiers relatifs non simultanément nuls on a :
▶ $\boldsymbol{\text{PGCD}(a,b) = \text{PGCD}(a,b-a) = \text{PGCD}(a-b,b)}$

**A09** On se propose de démontrer la formule de la soustraction.
*On montrerait facilement par disjonction de cas que l'on a les équivalences : $a$ et $b$ sont non simultanément nuls $\Leftrightarrow$ $a$ et $b-a$ sont non simultanément nuls $\Leftrightarrow$ $a-b$ et $b$ sont non simultanément nuls.*
On rappelle que, pour deux ensembles $E$ et $F$ on a l'équivalence :
$E = F \Leftrightarrow E \subset F$ et $F \subset E$.
Notons :
$\mathcal{D}(a,b)$ l'ensemble des diviseurs communs de $a$ et $b$ dans $\mathbb{Z}$,
$\mathcal{D}(a,b-a)$ l'ensemble des diviseurs communs de $a$ et $b-a$ dans $\mathbb{Z}$

1. Soit $d \in \mathcal{D}(a,b)$, montrer que $d \in \mathcal{D}(a,b-a)$, en déduire une inclusion.
2. Soit $d \in \mathcal{D}(a,b-a)$, montrer que $d \in \mathcal{D}(a,b)$, en déduire une inclusion.
3. Déduire de ce qui précède une égalité entre deux ensembles puis que : $\text{PGCD}(a,b) = \text{PGCD}(a,b-a)$.
4. Montrer que $\text{PGCD}(a,b) = \text{PGCD}(a-b,b)$.

**[D] Algorithme des soustractions pour obtenir le PGCD**

Elle consiste à appliquer plusieurs fois la formule de la soustraction et à utiliser à la fin le théorème « PGCD et divisibilité ».

**A10** À l'aide de la méthode de la soustraction, déterminer :
• $\text{PGCD}(75,60)$ • $\text{PGCD}(20,-35)$ • $\text{PGCD}(12,20)$

**A11** Soit $a$ un entier relatif, déterminer : $\text{PGCD}(a^2+1, a^2)$.

**A12** Soit $n \in \mathbb{N}$, déterminer : $\text{PGCD}(5^{2n}-1, 8)$.

**A13** Compléter le programme Python, la fonction pgcdsous retournant le PGCD de deux entiers naturels strictement positifs :

```
def pgcdsous(a,b:int):
    a, b = max(a, b), min(a, b)
    if a%b==0:
        return b
    else:
        return …
```

**[P]** Soient $a$ et $b$ deux entiers relatifs non simultanément nuls.
Pour tout entier relatif $k$, on a :
▶ $\boldsymbol{\text{PGCD}(a,b) = \text{PGCD}(a,b \pm ka) = \text{PGCD}(a \pm kb,b)}$
Autrement dit : dans le calcul du PGCD on peut ajouter/soustraire à l'un des nombres un multiple de l'autre nombre.

**A14** Soit $n \in \mathbb{N}$, déterminer :
$\text{PGCD}(2n+5, n+1)$ et $\text{PGCD}(3n+1, n+2)$

**P Théorème « PGCD et divisibilité »**

$a \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{Z}$, on a l'équivalence : ▶ $\boldsymbol{a|b \Leftrightarrow \mathrm{PGCD}(a,b) = |a|}$.

$a \in \mathbb{N} \setminus \{0\}$, $b \in \mathbb{Z}$, on a l'équivalence : ▶ $\boldsymbol{a|b \Leftrightarrow \mathrm{PGCD}(a,b) = a}$

**A08 On souhaite démontrer le théorème «PGCD et divisibilité».**
**On rappelle que, pour deux nombres $x$ et $y$ on a l'équivalence :**
**$x = y \Leftrightarrow x \leqslant y$ et $y \leqslant x$. Soient $a$ et $b$ deux entiers relatifs, $a \neq 0$.**

1. **Démontrons que : $a|b \Rightarrow \mathrm{PGCD}(a,b) = |a|$.**
   **On suppose que $a|b$.**
   a. **Montrer que $|a|$ est un diviseur commun de $a$ et $b$.**
   On procède par disjonction de cas suivant le signe de $a$ :
   • si $a > 0$, alors $|a| = a$, or $a|a$ donc $|a|$ divise $a$
   or, par hypothèse $a|b$ donc on a : $|a|$ divise $a$ et $a|b$ donc par transitivité $|a|$ divise $b$.
   Résumons : $|a|$ divise $a$ et divise $b$ donc $|a|$ est un diviseur commun de $a$ et $b$
   • si $a < 0$, alors $|a| = -a$, donc $|a|$ divise $-(-a)$ c'est-à-dire $a$, d'autre part $a|b$ donc $-a|b$ autrement dit $|a|$ divise $b$
   Résumons : $|a|$ divise $a$ et divise $b$ donc $|a|$ est un diviseur commun de $a$ et $b$
   Conclusion :
   pour tout $a \in \mathbb{Z} \setminus \{0\}$, $|a|$ est un diviseur commun de $a$ et $b$.

   **En déduire : $|a| \leqslant \mathrm{PGCD}(a,b)$.**
   $|a|$ est un diviseur commun de $a$ et $b$,
   $\mathrm{PGCD}(a,b)$ est le plus grand diviseur commun de $a$ et $b$ donc est supérieur ou égal à tout diviseur commun de $a$ et $b$, en particulier $\mathrm{PGCD}(a,b) \geqslant |a|$, i.e. $|a| \leqslant \mathrm{PGCD}(a,b)$.

   b. **En utilisant le fait que $\mathrm{PGCD}(a,b)$ est un diviseur de $a \neq 0$, justifier que $\mathrm{PGCD}(a,b) \leqslant |a|$.**
   On sait que, si $a \neq 0$ alors les diviseurs de $a$ sont compris entre $-|a|$ et $|a|$, donc : $-|a| \leqslant \mathrm{PGCD}(a,b) \leqslant |a|$, d'où : $\mathrm{PGCD}(a,b) \leqslant |a|$.

   c. **Conclure.**
   On a montré en **a.** que $|a| \leqslant \mathrm{PGCD}(a,b)$ et en **b.** que $\mathrm{PGCD}(a,b) \leqslant |a|$ donc $\mathrm{PGCD}(a,b) = |a|$.

   Pour $a \neq 0$ on a l'implication : $\boldsymbol{a|b \Rightarrow \mathrm{PGCD}(a,b) = |a|}$.

2. **Démontrons que : $\mathrm{PGCD}(a,b) = |a| \Rightarrow a|b$.**
   On suppose que : $\mathrm{PGCD}(a,b) = |a|$.
   $\mathrm{PGCD}(a,b)$ est un diviseur commun de $a$ et $b$.
   Or, $\mathrm{PGCD}(a,b) = |a|$, donc $|a|$ divise $a$ et divise $b$, en particulier $|a|$ divise $b$ $(*)$.
   On procède par disjonction de cas suivant le signe de $a$ :
   si $a > 0$, alors $|a| = a$ et il résulte de $(*)$ que $a|b$.
   si $a < 0$, alors $|a| = -a$ et il résulte de $(*)$ que $-a|b$ autrement dit que : $a|b$.
   Pour $a \neq 0$, on a l'implication : $\mathrm{PGCD}(a,b) = |a| \Rightarrow a|b$.

Conclusion
$a \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{Z}$, *on a l'équivalence :* $\boldsymbol{a|b \Leftrightarrow \mathrm{PGCD}(a,b) = |a|}$.
*La deuxième version du théorème est un corollaire en remarquant que, pour $a \in \mathbb{N}^*$, on a :* $|a| = a$.

**P** Pour $a$ et $b$ entiers relatifs non simultanément nuls on a :
▶ $\boldsymbol{\mathrm{PGCD}(a,b) = \mathrm{PGCD}(a,b-a) = \mathrm{PGCD}(a-b,b)}$

**A09 Démontrer la formule de la soustraction**.
$\mathcal{D}(a,b)$ l'ensemble des diviseurs communs de $a$ et $b$ dans $\mathbb{Z}$,
$\mathcal{D}(a,b-a)$ l'ensemble des diviseurs communs de $a$ et $b-a$ dans $\mathbb{Z}$

1. **Soit $d \in \mathcal{D}(a,b)$, montrer que $d \in \mathcal{D}(a,b-a)$, en déduire une inclusion.**
   $d \in \mathcal{D}(a,b)$ donc $d|a$ et $d|b$ donc $d$ divise toute combinaison linéaire de $a$ et $b$, en particulier $d|(-1)a + 1b$ i.e. $d|b-a$.
   On a donc : $d|a$ et $d|b-a$ donc $d \in \mathcal{D}(a,b-a)$.
   Résumons : si $d \in \mathcal{D}(a,b)$, alors $d \in \mathcal{D}(a,b-a)$.
   On en déduit : $\boldsymbol{\mathcal{D}(a,b) \subset \mathcal{D}(a,b-a)}$.

2. **Soit $d \in \mathcal{D}(a, b-a)$, montrer que $d \in \mathcal{D}(a, b)$, en déduire une inclusion.**
   $d \in \mathcal{D}(a, b-a)$ donc $d|a$ et $d|b-a$ donc $d$ divise toute combinaison linéaire de $a$ et $b-a$, en particulier :
   $d|1a + 1(b-a)$ i.e. $d|b$.
   On a donc : $d|a$ et $d|b$ donc $d \in \mathcal{D}(a, b)$.
   Résumons : si $d \in \mathcal{D}(a, b-a)$, alors $d \in \mathcal{D}(a, b)$.
   On en déduit : $\mathcal{D}(a, b-a) \subset \mathcal{D}(a, b)$.

3. **Déduire de ce qui précède une égalité entre deux ensembles puis que : $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a, b-a)$.**
   on a montré en 1. que : $\mathcal{D}(a, b) \subset \mathcal{D}(a, b-a)$
   et en 2. On a montré que : $\mathcal{D}(a, b-a) \subset \mathcal{D}(a, b)$.
   Il en résulte que : $\mathcal{D}(a, b) = \mathcal{D}(a, b-a)$.
   Remarquons d'abord que $\mathcal{D}(a, b)$ et $\mathcal{D}(a, b-a)$ contiennent 1 donc sont non vides, et qu'ils sont majorés, le premier par $\max\{|a|, |b|\}$, le second par $\max\{|a|, |b-a|\}$ donc ils admettent chacun un plus grand élément.
   Or, ces deux ensembles sont égaux, donc ils ont même plus grand élément, on a donc : $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a-b, b)$.

4. **Montrer que $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a-b, b)$.**
   On a :
   $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, a) = \mathrm{PGCD}(b, a-b)$ (d'après **3.**)
   $= \mathrm{PGCD}(a-b, b)$
   On a donc bien : $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a-b, b)$.

**D** **Algorithme des soustractions pour obtenir le PGCD**
Elle consiste à appliquer plusieurs fois la formule de la soustraction et à utiliser à la fin le théorème «PGCD et divisibilité».

**A10** **À l'aide de la méthode de la soustraction, déterminer :**
• $\mathrm{PGCD}(75, 60)$ • $\mathrm{PGCD}(20, -35)$ • $\mathrm{PGCD}(12, 20)$

• $\mathrm{PGCD}(75,60) = \mathrm{PGCD}(75-60,60) = \mathrm{PGCD}(15,60) = \mathbf{15}$ $(15|60)$

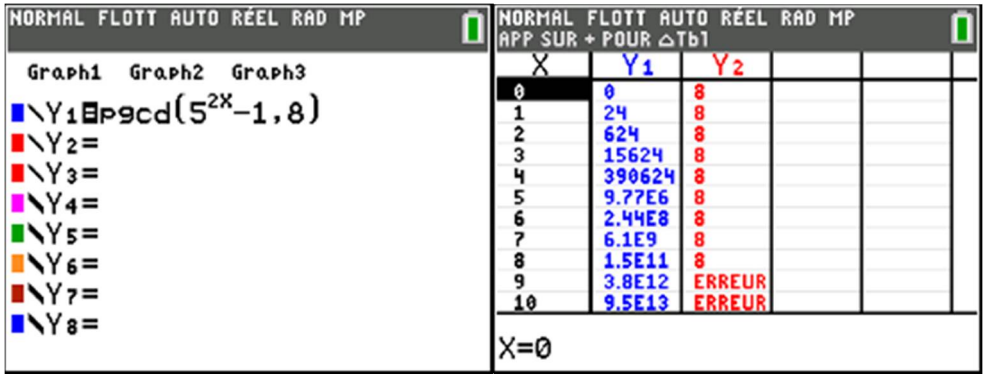
• $\mathrm{PGCD}(20,-35) = \mathrm{PGCD}(20,35) = \mathrm{PGCD}(20,35-20) = \mathrm{PGCD}(20,15)$
$= \mathrm{PGCD}(20-15,15) = \mathrm{PGCD}(5,15) = \mathbf{5}$ $(5|15)$

• $\mathrm{PGCD}(12,20) = \mathrm{PGCD}(12,20-12) = \mathrm{PGCD}(12,8) = \mathrm{PGCD}(12-8,8)$
$= \mathrm{PGCD}(4,8) = \mathbf{4}$ $(4|8)$

**A11** **Soit $a$ un entier relatif, déterminer : $\mathrm{PGCD}(a^2+1, a^2)$.**

$\mathrm{PGCD}(a^2+1, a^2) = \mathrm{PGCD}(a^2+1-a^2, a^2) = \mathrm{PGCD}(1, a^2) = 1$

**A12** **Soit $n \in \mathbb{N}$, déterminer : $\mathrm{PGCD}(5^{2n}-1, 8)$.**




On peut conjecturer que : $\forall n \in \mathbb{N}, \mathrm{PGCD}(5^{2n}-1, 8) = 8$.

Soit $n \in \mathbb{N}$, on a :
$5^{2n} - 1 = (5^2)^n - 1 = 25^n - 1 \equiv 1^n - 1 \equiv 1 - 1 \equiv 0\ [8]$
donc : $8|5^{2n}-1$, donc d'après le théorème PGCD et divisibilité on en déduit que : $\mathrm{PGCD}(5^{2n}-1, 8) = 8$.

Conclusion : $\forall n \in \mathbb{N}, \mathrm{PGCD}(5^{2n}-1, 8) = 8$.

$P$ Soient $a$ et $b$ deux entiers relatifs non simultanément nuls.
Pour tout entier relatif $k$, on a :

▶ $\mathbf{PGCD}(a,b) = \mathbf{PGCD}(a, b \pm ka) = \mathbf{PGCD}(a \pm kb, b)$

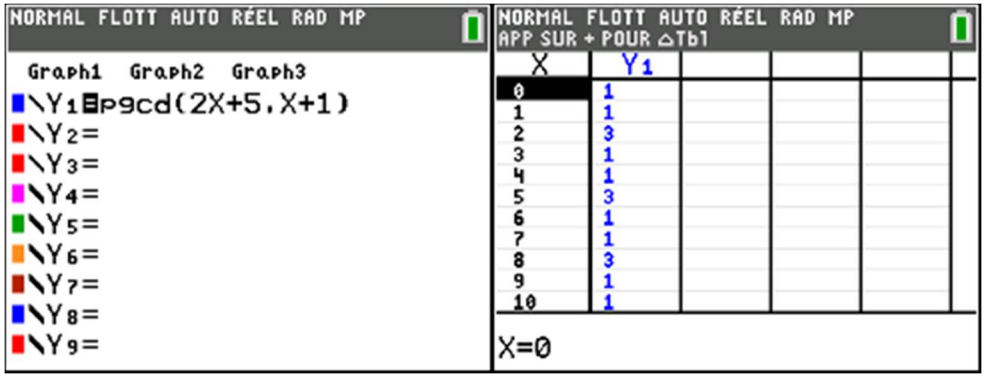
Autrement dit dans le calcul du PGCD on peut ajouter/soustraire à l'un des nombres un multiple de l'autre nombre.

**A13 Compléter le programme Python, la fonction pgcdsous retournant le PGCD de deux entiers naturels strictement positifs :**

```
def pgcdsous(a,b:int):
    a, b = max(a, b), min(a, b)
    if a%b==0:
        return b
    else:
        return pgcdsous(a-b,b)
```

**A14 $n \in \mathbb{N}$, $\mathbf{PGCD}(2n+5, n+1)$ et $\mathbf{PGCD}(3n+1, n+2)$**

☐ $\mathbf{PGCD}(2n+5, n+1)$



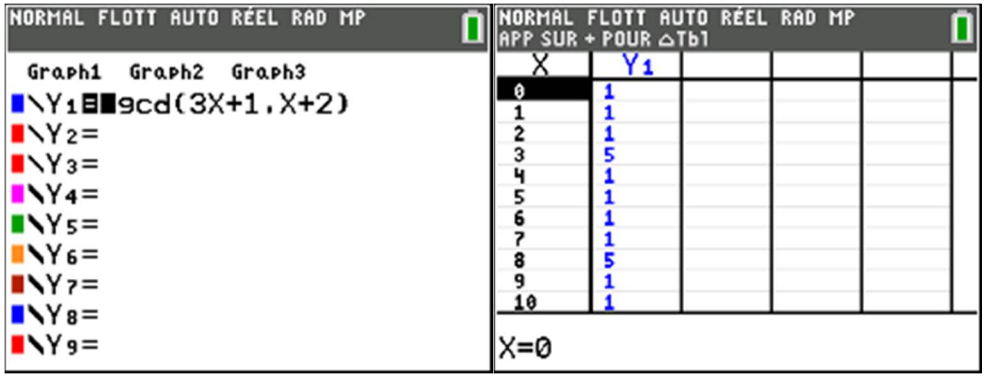

Soit $n \in \mathbb{N}$, on a :
$\mathrm{PGCD}(2n+5, n+17) = \mathrm{PGCD}(2n+5-2(n+1), n+1)$
$= \mathrm{PGCD}(3, n+1)$
Pour tout $n \in \mathbb{N}, \mathrm{PGCD}(2n+5, n+17) = \mathrm{PGCD}(3, n+1)$.

On procède par disjonction de cas suivant le reste modulo 3 de $n$

- si $n \equiv 0\ [3]$, alors il existe $k \in \mathbb{N}$ tel que $n = 3k$ et on a :
  $\mathrm{PGCD}(3, n+1) = \mathrm{PGCD}(3, 3k+1) = \mathrm{PGCD}(3, 3k+1-k\times 3)$
  $= \mathrm{PGCD}(3,1) = 1$
- si $n \equiv 1\ [3]$, alors il existe $k \in \mathbb{N}$ tel que $n = 3k+1$ et on a :
  $\mathrm{PGCD}(3, n+1) = \mathrm{PGCD}(3, 3k+1+1) = \mathrm{PGCD}(3, 3k+2)$
  $= \mathrm{PGCD}(3, 3k+2-k\times 3) = \mathrm{PGCD}(3,2) = \mathrm{PGCD}(3-2, 2)$
  $= \mathrm{PGCD}(1,2) = 1$
- si $n \equiv 2\ [3]$, alors il existe $k \in \mathbb{N}$ tel que $n = 3k+2$ et on a :
  $\mathrm{PGCD}(3, n+1) = \mathrm{PGCD}(3, 3k+2+1) = \mathrm{PGCD}(3, 3k+3)$
  $= \mathrm{PGCD}(3, 3k+3-k\times 3) = \mathrm{PGCD}(3,3) = 3$ $(3|3)$

Conclusion
**si $n \equiv 2\ [3]$, alors $\mathbf{PGCD}(2n+5, n+1) = 3$**
**si $n \not\equiv 2\ [3]$, alors $\mathbf{PGCD}(2n+5, n+1) = 1$**

☐ $\mathbf{PGCD}(3n+1, n+2)$




Soit $n \in \mathbb{N}$, on a :
$\mathrm{PGCD}(3n+1, n+2) = \mathrm{PGCD}(3n+1-3(n+2), n+2)$
$= \mathrm{PGCD}(3n+1-3n-6, n+2) = \mathrm{PGCD}(-5, n+2)$
$= \mathrm{PGCD}(5, n+2)$
Pour tout $n \in \mathbb{N}, \mathrm{PGCD}(3n+1, n+2) = \mathrm{PGCD}(5, n+2)$.

On procède par disjonction de cas suivant le reste modulo 5 de $n$ :

- si $n \equiv 0\ [5]$, alors il existe $k \in \mathbb{N}, n = 5k$
  $\mathrm{PGCD}(5, n+2) = \mathrm{PGCD}(5, 5k+2) = \mathrm{PGCD}(5, 5k+2-k\times 5)$
  $= \mathrm{PGCD}(5, 2) = \mathrm{PGCD}(5-2\times 2, 2) = \mathrm{PGCD}(1, 2) = 1$
- si $n \equiv 1\ [5]$, alors il existe $k \in \mathbb{N}, n = 5k+1$
  $\mathrm{PGCD}(5, n+2) = \mathrm{PGCD}(5, 5k+1+2) = \mathrm{PGCD}(5, 5k+3)$
  $= \mathrm{PGCD}(5, 5k+3-k\times 5) = \mathrm{PGCD}(5, 3) = \mathrm{PGCD}(5-3, 3)$
  $= \mathrm{PGCD}(2, 3) = \mathrm{PGCD}(2, 3-2) = \mathrm{PGCD}(2, 1) = 1$
- si $n \equiv 2\ [5]$, alors il existe $k \in \mathbb{N}, n = 5k+2$
  $\mathrm{PGCD}(5, n+2) = \mathrm{PGCD}(5, 5k+2+2) = \mathrm{PGCD}(5, 5k+4)$
  $= \mathrm{PGCD}(5, 5k+4-k\times 5) = \mathrm{PGCD}(5, 4) = \mathrm{PGCD}(5-4, 4)$
  $= \mathrm{PGCD}(1, 4) = 1$
- si $n \equiv 3\ [5]$, alors il existe $k \in \mathbb{N}, n = 5k+3$
  $\mathrm{PGCD}(5, n+2) = \mathrm{PGCD}(5, 5k+3+2) = \mathrm{PGCD}(5, 5k+5)$
  $= \mathrm{PGCD}(5, 5k+5-5k) = \mathrm{PGCD}(5,5) = 5\ (5|5)$
- si $n \equiv 4\ [5]$, alors il existe $k \in \mathbb{N}, n = 5k+4$
  $\mathrm{PGCD}(5, n+2) = \mathrm{PGCD}(5, 5k+4+2) = \mathrm{PGCD}(5, 5k+6)$
  $= \mathrm{PGCD}(5, 5k+6-k\times 5) = \mathrm{PGCD}(5, 6) = \mathrm{PGCD}(5,6-5)$
  $= \mathrm{PGCD}(5,1) = 1$

Conclusion

**si $n \equiv 3\ [5]$, alors $\mathrm{PGCD}(3n+1, n+2) = 5$**
**si $n \not\equiv 3\ [5]$, alors $\mathrm{PGCD}(3n+1, n+2) = 1$**

**F Formule de l'addition**

Soit $a$ et $b$ deux entiers relatifs non simultanément nuls.

On a :

$$\blacktriangleright \ \mathrm{PGCD}(a,b) = \mathrm{PGCD}(a,b+a) = \mathrm{PGCD}(a+b,a)$$

**A15** Démontrer la formule d'addition à partir de la formule de la soustraction.

**A16** On se propose de démontrer les formules admises jusqu'ici, valables pour $a$ et $b$ entiers relatifs non simultanément nuls et $n$ entier naturel :

$$\mathrm{PGCD}(a,b) = \mathrm{PGCD}(a,b+na) = \mathrm{PGCD}(a,b-na)$$
$$\mathrm{PGCD}(a,b) = \mathrm{PGCD}(a+nb,b) = \mathrm{PGCD}(a-nb,b)$$

On pourra utiliser les formules élémentaires sur le PGCD, la formule de la soustraction et la formule d'addition.

1. Démontrer que : $\forall n \in \mathbb{N}, \mathrm{PGCD}(a,b) = \mathrm{PGCD}(a,b+na)$.
2. En déduire que : $\forall n \in \mathbb{N}, \mathrm{PGCD}(a,b) = \mathrm{PGCD}(a,b-na)$.
3. Démontrer les deux dernières formules.

**F Formule du reste**

Pour $a$ et $b$ entiers relatifs, $b \neq 0$, on note $r$ le reste de la division euclidienne de $a$ par $b$, alors :

$$\blacktriangleright \ \mathbf{PGCD}(\boldsymbol{a},\boldsymbol{b}) = \mathbf{PGCD}(\boldsymbol{b},\boldsymbol{r})$$

**A17** Démontrer la formule du reste.

**A18** Déterminer $\mathrm{PGCD}(456,25)$, $\mathrm{PGCD}(7,120)$ et $\mathrm{PGCD}(439,50)$.

**A19** Soit $n \in \mathbb{N}$, déterminer $\mathrm{PGCD}(3n+4,2n+1)$.

**A20** Soit $n \in \mathbb{N}$, déterminer $\mathrm{PGCD}(2n^2-n-15,n-3)$.

**A21** Création élève

**A22** Création élève

**A15 Démontrer la formule d'addition.**

Soient $a$ et $b$ deux entiers relatifs non simultanément nuls, on a :

$$\begin{aligned}&\mathrm{PGCD}(a,b+a)\\ &= \mathrm{PGCD}(a,b+a-a) \quad (formule\ de\ la\ soustraction)\\ &= \mathrm{PGCD}(a,b)\end{aligned}$$

On a donc : $\mathbf{PGCD}(\boldsymbol{a},\boldsymbol{b}) = \mathbf{PGCD}(\boldsymbol{a},\boldsymbol{b}+\boldsymbol{a})$. De même :

$$\begin{aligned}&\mathrm{PGCD}(a+b,b)\\ &= \mathrm{PGCD}(a+b-b,b) \quad (formule\ de\ la\ soustraction)\\ &= \mathrm{PGCD}(a,b)\end{aligned}$$

On a donc : $\mathbf{PGCD}(\boldsymbol{a},\boldsymbol{b}) = \mathbf{PGCD}(\boldsymbol{a}+\boldsymbol{b},\boldsymbol{b})$.

**A16 On se propose de démontrer les formules admises jusqu'ici, valables pour $\boldsymbol{a}$ et $\boldsymbol{b}$ entiers relatifs non simultanément nuls et $\boldsymbol{n}$ entier naturel :**

$$\mathbf{PGCD}(\boldsymbol{a},\boldsymbol{b}) = \mathbf{PGCD}(\boldsymbol{a},\boldsymbol{b}+\boldsymbol{na}) = \mathbf{PGCD}(\boldsymbol{a},\boldsymbol{b}-\boldsymbol{na})$$
$$\mathbf{PGCD}(\boldsymbol{a},\boldsymbol{b}) = \mathbf{PGCD}(\boldsymbol{a}+\boldsymbol{nb},\boldsymbol{b}) = \mathbf{PGCD}(\boldsymbol{a}-\boldsymbol{nb},\boldsymbol{b})$$

**On pourra utiliser les formules élémentaires sur le PGCD, la formule de la soustraction et la formule d'addition.**

1. **Démontrer que : $\forall \boldsymbol{n} \in \mathbb{N}, \mathbf{PGCD}(\boldsymbol{a},\boldsymbol{b}) = \mathbf{PGCD}(\boldsymbol{a},\boldsymbol{b}+\boldsymbol{na})$.**

Pour tout $n \in \mathbb{N}$ on considère la proposition

$$P_n : \text{« } \mathrm{PGCD}(a,b) = \mathrm{PGCD}(a,b+na) \text{ »}$$

• **initialisation**

Si $n = 0$, on a : $\mathrm{PGCD}(a,b+0\times a) = \mathrm{PGCD}(a,b)$, $P_0$ est vraie.

• **hérédité**

Soit $k \in \mathbb{N}$ tel que $P_k$ est vraie et montrons que $P_{k+1}$ est vraie.

$$\begin{aligned}&\mathrm{PGCD}(a,b+(k+1)a) = \mathrm{PGCD}(a,b+ka+a)\\ &= \mathrm{PGCD}(a,b+ka+a-a) = \mathrm{PGCD}(a,b+ka) = \mathrm{PGCD}(a,b)\end{aligned}$$

On a donc : $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(a,b+(k+1)a)$

autrement dit $P_{k+1}$ est vraie.

Conclusion

Il résulte des deux points précédents et du principe de récurrence que, pour tout $n \in \mathbb{N}$, $P_n$ est vraie autrement dit :

$$\forall n \in \mathbb{N}, \mathrm{PGCD}(a,b) = \mathrm{PGCD}(a,b+na)$$

**2. En déduire que : $\forall n \in \mathbb{N}$, $\mathbf{PGCD}(a,b) = \mathbf{PGCD}(a, b-na)$.**

On a :

$$\mathrm{PGCD}(a, b-na) = \mathrm{PGCD}(a, b-na+na) = \mathrm{PGCD}(a,b)$$

On a donc bien : $\mathbf{PGCD}(a,b) = \mathbf{PGCD}(a, b-na)$.

**3. • montrons que $\mathbf{PGCD}(a,b) = \mathbf{PGCD}(a+nb, b)$.**

On a :

$$\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,a) = \mathrm{PGCD}(b, a+nb)$$
$$= \mathrm{PGCD}(a+nb, b)$$

Résumons : $\mathbf{PGCD}(a,b) = \mathbf{PGCD}(a+nb, b)$

**• montrons que : $\mathbf{PGCD}(a,b) = \mathbf{PGCD}(a-nb, b)$.**

On a :

$$\mathrm{PGCD}(a-nb, b) = \mathrm{PGCD}(b, a-nb) = \mathrm{PGCD}(b, a-nb+nb)$$
$$= \mathrm{PGCD}(b,a) = \mathrm{PGCD}(a,b)$$

Résumons : $\mathbf{PGCD}(a,b) = \mathbf{PGCD}(a-nb, b)$.

**$F$ Formule du reste**

Pour $a$ et $b$ entiers relatifs, $b \neq 0$, on note $r$ le reste de la division euclidienne de $a$ par $b$, alors : ▶ $\mathbf{PGCD}(a,b) = \mathbf{PGCD}(b,r)$

**A17 Démontrer la formule du reste.**

$a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$ donc il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que :

$$a = qb + r, \text{ avec } 0 \leqslant r < |b|$$

On en déduit : $r = a - qb$. On a :

$$\mathrm{PGCD}(a,b) = \mathrm{PGCD}(qb+r, b) = \mathrm{PGCD}(qb+r-qb, b)$$
$$= \mathrm{PGCD}(r,b) = \mathrm{PGCD}(b,r)$$

Conclusion : $\mathrm{PGCD}(r,b) = \mathrm{PGCD}(b,r)$.

**A18 $\mathbf{PGCD}(456,25)$, $\mathbf{PGCD}(7,120)$ et $\mathbf{PGCD}(439,50)$**

• La division euclidienne de 456 par 25 donne :

$$456 = 18 \times 25 + 6 \text{ avec } 0 \leqslant 6 < 25$$

donc : $\mathrm{PGCD}(456,25) = \mathrm{PGCD}(25,6) = \mathrm{PGCD}(25 - 4 \times 6, 6)$

$= \mathrm{PGCD}(1,6) = 1$

Finalement : $\mathbf{PGCD}(456,25) = \mathbf{1}$.

• La division euclidienne de 120 par 7 donne :

$120 = 17 \times 7 + 1$ avec $0 \leqslant 1 < 7$.

On a : $\mathrm{PGCD}(120,7) = \mathrm{PGCD}(7,1) = 1$

Finalement : $\boldsymbol{PGCD}(\mathbf{120},\mathbf{7}) = \mathbf{1}$.

**A19** Soit $n \in \mathbb{N}$, déterminer $\mathrm{PGCD}(3n+4, 2n+1)$.

$$\mathrm{PGCD}(3n+4, 2n+1)$$
$$= \mathrm{PGCD}(3n+4-(2n+1), 2n+1)$$
$$= \mathrm{PGCD}(3n+4-2n-1, 2n+1)$$
$$= \mathrm{PGCD}(n+3, 2n+1)$$
$$= \mathrm{PGCD}(n+3, 2n+1-2(n+3))$$
$$= \mathrm{PGCD}(n+3, 2n+1-2n-6)$$
$$= \mathrm{PGCD}(n+3, -5)$$
$$= \mathrm{PGCD}(n+3, 5)$$

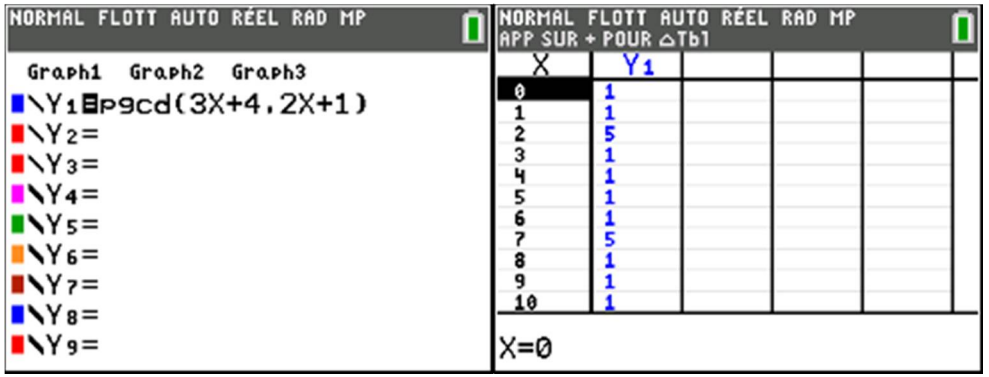
Ensuite on procède par disjonction de cas suivant le reste modulo 5 de $n$ et on obtient (non rédigé) :

si $n \equiv 2\ [5]$ alors $\mathrm{PGCD}(n+3,5) = 5$, sinon $\mathrm{PGCD}(n+3,5) = 1$.

Conclusion

**si $\boldsymbol{n \equiv 2\ [5]}$ alors $\mathbf{PGCD}(\mathbf{3n+4}, \mathbf{2n+1}) = \mathbf{5}$,**

**sinon $\mathbf{PGCD}(\mathbf{3n+4}, \mathbf{2n+1})$.**



**A20** **Soit $n \in \mathbb{N}$, déterminer $\mathrm{PGCD}(2n^2 - n - 15, n - 3)$.**

Examinons d'abord si les nombres $2n^2 - n - 15$ et $n - 3$ peuvent être simultanément nuls :

$$\begin{cases} 2n^2 - n - 15 = 0 \\ n - 3 = 0 \end{cases} \Leftrightarrow \begin{cases} n = 3 \\ 2(3)^2 - 3 - 15 = 0 \end{cases} \Leftrightarrow \begin{cases} n = 3 \\ 0 = 0 \end{cases} \Leftrightarrow n = 3$$

Le $\mathrm{PGCD}(2n^2 - n - 15, n - 3)$ existe si et seulement si $n \neq 3$.

Pour tout $n \in \mathbb{N}$, on a : $2n^2 - n - 15 = (n - 3)(2n + 5)$.

Pour $n \neq 3$, on a :

$$\mathrm{PGCD}(2n^2 - n - 15, n - 3) = \mathrm{PGCD}((n - 3)(2n + 5), n - 3)$$
$$= |n - 3| \quad (n - 3 | (n - 3)(2n + 5))$$

Conclusion :

• si $n = 3$ alors les nombres $2n^2 - n - 15$ et $n - 3$ n'admettent pas de PGCD

• si $n \neq 3$, alors $\mathrm{PGCD}(2n^2 - n - 15, n - 3) = |n - 3|$

**A21** Création élève

**[P] Algorithme d'Euclide**

Soient $a$ et $b$ deux entiers naturels tels que $a > b > 0$, on souhaite déterminer $\text{PGCD}(a,b)$.

• $r_1$ est le reste de la division euclidienne de $a$ par b :

$$\text{PGCD}(a,b) = \text{PGCD}(b,r_1)$$

si $r_1 = 0$ on s'arrête et :

$$\text{PGCD}(a,b) = \text{PGCD}(b,r_1 = 0) = b$$

sinon :

• $r_2$ est le reste de la division euclidienne de $b$ par $r_1$

si $r_2 = 0$ on s'arrête et :

$$\text{PGCD}(a,b) = \text{PGCD}(b,r_1) = \text{PGCD}(r_1,r_2 = 0) = r_1$$

donc **$\text{PGCD}(a,b)$ est égal au dernier reste non nul**

sinon :

• $r_3$ est le reste de la division euclidienne de $r_1$ par $r_2$

si $r_2 = 0$ on s'arrête et :

$$\text{PGCD}(a,b) = \text{PGCD}(b,r_1) = \text{PGCD}(r_1,r_2) = \text{PGCD}(r_2,r_3 = 0) = r_2$$

donc **$\text{PGCD}(a,b)$ est égal au dernier reste non nul**

etc..

On obtient un nombre fini d'entiers naturels $r_1 > r_2 > \cdots$, le dernier étant zéro, et :

▶ **$\text{PGCD}(a,b)$ est égal au dernier reste non nul**

**A22** À l'aide de l'algorithme d'Euclide déterminer $\text{PGCD}(108,40)$.

**A23** À l'aide de l'algorithme d'Euclide déterminer $\text{PGCD}(439,50)$.

[D] On dit que deux entiers relatifs non simultanément nuls sont **premiers entre eux** lorsque leur **PGCD est 1**.

Pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ non simultanément nuls :

$$a \text{ et } b \text{ sont premiers entre eux} \overset{déf}{\Leftrightarrow} \text{PGCD}(a,b) = 1$$

```
1 def pgcd_Euclide(a,b):
2     while b!=0:
3         r=a%b
4         a,b=b,r
5     return a
```

Programme utilisable sur la TI83

**A24** 317 et 25 sont-ils premiers entre eux ? 95 et $(-255)$ ?

💣 Ne pas confondre « les deux nombres sont **premiers entre eux** » avec « les deux nombres sont **premiers** ».

**A25** On cherche à trouver un couple $(x_0,y_0)$ d'entiers relatifs, s'il en existe, tel que : $46x_0 + 21y_0 = 1$.

À l'aide de l'algorithme d'Euclide, montrer que 46 et 21 sont premiers entre eux puis déterminer un tel couple $(x_0,y_0)$.

[i] On vient de trouver une solution particulière $(x_0,y_0)$ de l'équation $46x_0 + 21y_0 = 1$, avec $(x,y) \in \mathbb{Z}^2$.

**A26 [avec calculatrice]** On cherche à trouver un couple $(x_0,y_0)$ d'entiers relatifs, s'il en existe, tel que : $359x_0 + 450y_0 = 1$.

À l'aide de l'algorithme d'Euclide, montrer que 359 et 450 sont premiers entre eux puis déterminer un tel couple $(x_0,y_0)$.

**A27 [avec calculatrice]**

Existe-il $(x_0,y_0) \in \mathbb{Z}^2$ tel que : $731x_0 + 272y_0 = 1$ ?

[P] Pour $a$ et $b$ entiers relatifs non simultanément nuls et $k$ entier relatif non nul, on a :

▶ $\text{PGCD}(k \times a, k \times b) = |k| \times \text{PGCD}(a,b)$

**A28** Démontrer la propriété précédente.

**A29** Déterminer $\text{PGCD}(300,700)$, $\text{PGCD}(2^{50},2^{51})$.

**A22 À l'aide de l'algorithme d'Euclide déterminer $\mathbf{PGCD(108,40)}$.**

Appliquons l'algorithme d'Euclide :

| | |
|---|---|
| | $a = 108$ |
| | $b = 40$ |
| $108 = 2 \times 40 + 28$ | $r_1 = 28$ |
| $40 = 1 \times 28 + 12$ | $r_2 = 12$ |
| $28 = 2 \times 2 + 4$ | $r_3 = 4$ |
| $12 = 3 \times 4 + 0$ | $r_4 = 0$ |

Le dernier reste non nul est 4 donc : $\mathbf{PGCD(108,40) = 4}$.

**A23 À l'aide de l'algorithme d'Euclide déterminer $\mathbf{PGCD(439,50)}$.**

Appliquons l'algorithme d'Euclide :

| | |
|---|---|
| | $a = 439$ |
| | $b = 50$ |
| $439 = 8 \times 50 + 39$ | $r_1 = 39$ |
| $50 = 1 \times 39 + 11$ | $r_2 = 11$ |
| $39 = 3 \times 11 + 6$ | $r_3 = 6$ |
| $11 = 1 \times 6 + 5$ | $r_4 = 5$ |
| $6 = 1 \times 5 + 1$ | $r_5 = 1$ |
| $5 = 5 \times 1 + 0$ | $r_6 = 0$ |

Le dernier reste non nul est 1 donc : $\mathbf{PGCD(439,50) = 1}$.

$D$ On dit que deux entiers relatifs non simultanément nuls sont **premiers entre eux** lorsque leur **PGCD est 1**.
Pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ non simultanément nuls :

$$a \text{ et } b \text{ sont } \textbf{premiers entre eux} \overset{déf}{\Leftrightarrow} \mathrm{PGCD}(a,b) = 1$$

**A24 • 317 et 25 sont-ils premiers entre eux ?**

$\mathrm{PGCD}(317,25) = \mathrm{PGCD}(317 - 12 \times 25,25)$
$= \mathrm{PGCD}(17,25) = \mathrm{PGCD}(17,25 - 17) = \mathrm{PGCD}(17,8)$
$= \mathrm{PGCD}(17 - 2 \times 8,8) = \mathrm{PGCD}(1,8) = 1$

$\mathrm{PGCD}(317,25) = 1$ donc **317 et 25 sont premiers entre eux**.

On peut aussi déterminer $\mathrm{PGCD}(317,25)$ par l'algorithme d'Euclide, non rédigée ici (les restes successifs sont 17, 8, 1 et 0).

**• 95 et $(-255)$ sont-ils premiers entre eux ?**

$5|95$ et $5|(-255)$ donc 5 appartient à la liste des diviseurs communs de 95 et $(-255)$ par conséquent $\mathrm{PGCD}(95,-255) \geqslant 5$ donc $\mathrm{PGCD}(95,-255) \neq 1$ : les nombres 95 et $(-255)$ ne sont pas premiers entre eux.

Autre méthode

On peut remarquer que $\mathrm{PGCD}(95,-255) = \mathrm{PGCD}(95,255)$ puis calculer simplement ce dernier par une méthode habituelle et remarquer que $\mathrm{PGCD}(95,255) \neq 1$.

**A25 On cherche à trouver un couple $(x_0, y_0)$ d'entiers relatifs, s'il en existe, tel que : $46x_0 + 21y_0 = 1$.**
**À l'aide de l'algorithme d'Euclide, montrer que 46 et 21 sont premiers entre eux puis déterminer un tel couple $(x_0, y_0)$.**

Appliquons l'algorithme d'Euclide :

| | |
|---|---|
| | $a = 46$ |
| | $b = 21$ |
| $46 = 2 \times 21 + 4$ | $r_1 = 4$ |
| $21 = 5 \times 4 + 1$ | $r_2 = 1$ |
| $4 = 4 \times 1 + 0$ | $r_3 = 0$ |

Le dernier reste non nul est 1 donc $\mathrm{PGCD}(46,21) = 1$,
par conséquent **46 et 21 sont premiers entre eux**.

On a :
$21 - 5 \times 4 = 1$
$21 - 5(46 - 2 \times 21) = 1$
$21 - 5 \times 46 + 10 \times 21 = 1$
$11 \times 21 - 5 \times 46 = 1$
$46 \times (-5) + 11 \times 21 = 1$
Donc : $\mathbf{(x_0, y_0) = (-5, 11)}$ **est un couple solution.**
L'équation admet d'autres couples solutions.

**A26** **On cherche à trouver un couple $(x_0, y_0)$ d'entiers relatifs, s'il en existe, tel que : $359x_0 + 450y_0 = 1$.**
**À l'aide de l'algorithme d'Euclide, montrer que $359$ et $450$ sont premiers entre eux puis déterminer un tel couple $(x_0, y_0)$.**

Appliquons l'algorithme d'Euclide :

| | |
|---|---|
| | $a = 450$ |
| | $b = 359$ |
| $450 = 1 \times 359 + 91$ | $r_1 = 91$ |
| $359 = 3 \times 91 + 86$ | $r_2 = 86$ |
| $91 = 1 \times 86 + 5$ | $r_3 = 5$ |
| $86 = 17 \times 5 + 1$ | $r_4 = 1$ |
| $5 = 5 \times 1 + 0$ | $r_0 = 0$ |

Le PGCD est le dernier reste non nul, $\mathrm{PGCD}(450, 359) = 1$
donc **$450$ et $359$ sont premiers entre eux**.

On a :
$86 - 17 \times 5 = 1$
$86 - 17 \times (91 - 1 \times 86) = 1$
$86 - 17 \times 91 + 17 \times 86 = 1$
$18 \times 86 - 17 \times 91 = 1$
$18 \times (359 - 3 \times 91) - 17 \times 91 = 1$
$18 \times 359 - 54 \times 91 - 17 \times 91 = 1$
$18 \times 359 - 71 \times 91 = 1$
$18 \times 359 - 71 \times (450 - 1 \times 359) = 1$
$18 \times 359 - 71 \times 450 + 71 \times 359 = 1$
$89 \times 359 - 71 \times 450 = 1$
$359 \times 89 + 450 \times (-71) = 0$
Donc : $(x_0, y_0) = (89, -71)$ est un couple solution.
L'équation admet d'autres couples solutions.

**A27** **Existe-il $(x_0, y_0) \in \mathbb{Z}^2$ tel que : $731u_0 + 272v_0 = 1$ ?**

Appliquons l'algorithme d'Euclide pour déterminer $\mathrm{PGCD}(731,272)$ :

| | |
|---|---|
| | $a = 731$ |
| | $b = 272$ |
| $731 = 2 \times 272 + 187$ | $r_1 = 187$ |
| $272 = 1 \times 187 + 85$ | $r_2 = 85$ |
| $187 = 2 \times 85 + 17$ | $r_3 = 17$ |
| $86 = 5 \times 17 + 0$ | $r_4 = 0$ |

Le dernier reste non nul est $17$ donc $\mathrm{PGCD}(731, 272) = 17$.

Supposons qu'il existe $(x_0, y_0) \in \mathbb{Z}^2$ tel que : $731x_0 + 272y_0 = 1$.
On a : $17|731$ et $17|272$ donc $17$ divise toute combinaison linéaire de $731$ et $272$, en particulier $17|731x_0 + 272y_0$,
Or, $731x_0 + 272y_0 = 1$ donc $17|1$ ce qui est FAUX, par conséquent il faut rejeter l'hypothèse d'existence d'un tel couple $(x_0, y_0)$.

Conclusion : **il n'existe pas** $(x_0, y_0) \in \mathbb{Z}^2$ tq : $731x_0 + 272y_0 = 1$.

$P$ Pour $a$ et $b$ entiers relatifs non simultanément nuls et $k$ entier relatif non nul, on a :
▶ $\mathrm{PGCD}(k \times a, k \times b) = |k| \times \mathrm{PGCD}(a, b)$

**A28** **Justification de la propriété précédente.**
$a \in \mathbb{Z}, b \in \mathbb{Z}$ sont non simultanément nuls, $k \neq 0$

☐ **on suppose $k > 0$**
On procède par disjonction de cas suivant que $b$ est, ou non, nul.

• si $b = 0$
On a :
$\mathrm{PGCD}(ka, k0) = \mathrm{PGCD}(ka, 0) = k \times |a| = |k| \times \mathrm{PGCD}(a, 0)$
donc l'égalité est vraie.
• si $b \neq 0$
La division euclidienne de $a$ par $b$ donne $a = qb + r_1$, $0 \leqslant r_1 < |b|$,
notons $r_p$ le dernier reste non nul dans les divisions successives.
On a : $r_p \neq 0$, $r_{p+1} = 0$ et $r_p = \mathrm{PGCD}(a, b)$, et :
$|b| > r_2 > \cdots > r_p > r_{p+1}(= 0)$

La division euclidienne de $ka$ par $kb$ peut se déduire de celle de $a$ par $b$ et on obtient : $ka = k(qb + r_1) = q(kb) + kr_1, 0 \leqslant kr_1 < kb$ donc le reste de la division euclidienne de $ka$ par $kb$ est $kr_1$.
On montrerait de proche en proche que la liste des restes obtenus en appliquant l'algorithme d'Euclide pour obtenir $\text{PGCD}(ka, kb)$ est $kr_1, kr_2, \ldots, kr_p$ et $kr_{p+1}$ avec $kr_p \neq 0$ et $kr_{p+1} = k \times 0 = 0$
ce qui montre que $\text{PGCD}(ka, kb) = kr_p = k \times \text{PGCD}(a, b)$.
On a : $\text{PGCD}(ka, kb) = k \times \text{PGCD}(a, b)$, et comme $k > 0$ il est égal à sa valeur absolue donc l'égalité précédente s'écrit aussi :

$$\text{PGCD}(k \times a, k \times b) = |k| \times \text{PGCD}(a, b)$$

☐ **on suppose $k < 0$**
Rappelons que le PGCD de deux nombres est égal à celui de leurs valeurs absolues $(*)$, et que la valeur absolue d'un produit est égal au produit des valeurs absolues $(**)$.
On a :

$$\begin{aligned}
&\text{PGCD}(ka, kb) \\
&= \text{PGCD}(|k \times a|, |k \times b|) && \text{(d'après } (*)) \\
&= \text{PGCD}(|k| \times |a|, |k| \times |b|) && \text{(d'après } (**)) \\
&= |k| \times \text{PGCD}(|a|, |b|) && \text{(en utilisant le cas précédent)}
\end{aligned}$$

Donc : $\text{PGCD}(k \times a, k \times b) = |k| \times \text{PGCD}(a, b)$.

**A29** • $\mathbf{PGCD(300, 700)}$

On a :

$$\begin{aligned}
&\text{PGCD}(300,700) \\
&= \text{PGCD}(100 \times 3,100 \times 7) \\
&= |100| \times \text{PGCD}(3,7) \\
&= 100 \times \text{PGCD}(3,7 - 2 \times 3) \\
&= 100 \times \text{PGCD}(3,1) \\
&= 100 \times 1 \\
&= 100
\end{aligned}$$

Conclusion : $\mathbf{PGCD(300, 700) = 100}$.

• $\mathbf{PGCD(2^{50}, 2^{51})}$
On a :

$$\begin{aligned}
&\text{PGCD}(2^{50}, 2^{51}) \\
&= \text{PGCD}(2^{50}, 2^{50} \times 2^1) \\
&= \text{PGCD}(2^{50} \times 1, 2^{50} \times 2) \\
&= |2^{50}| \times \text{PGCD}(1,2) \\
&= 2^{50} \times 1 \\
&= 2^{50}
\end{aligned}$$

Conclusion : $\mathbf{PGCD\left(2^{50}, 2^{51}\right) = 2^{50}}$.

$P$ Pour $a$ et $b$ entiers relatifs non simultanément nuls, on note $a'$ et $b'$ les entiers relatifs tels que :

$$a = a' \times \text{PGCD}(a, b)$$
$$b = b' \times \text{PGCD}(a, b)$$

alors $a'$ et $b'$ sont nécessairement premiers entre eux.

**A30** Démontrer la propriété précédente.

$P$ Soient $a$ et $b$ des entiers relatifs non simultanément nuls, $a'$, $b'$ des entiers relatifs **premiers entre eux** et $d$ un entier naturel tels que :

$$a = a' \times d$$
$$b = b' \times d$$

alors $d$ est le PGCD de $a$ et $b$.

**A31** Démontrer la propriété précédente.

**A32** Déterminer tous les $(a, b)$ d'entiers naturels non nuls tels que :

$$\begin{cases} a \times b = 150 \\ \text{PGCD}(a, b) = 5 \end{cases}$$

$P$ ▶**Théorème de Bézout**

Soient $a$ et $b$ deux entiers relatifs non simultanément nuls, on a l'équivalence :

$a$ et $b$ sont **premiers entre eux** ⇔ il existe deux entiers relatifs $u$ et $v$ tels que : $\boldsymbol{au + bv = 1}$

autrement dit :

deux entiers relatifs non simultanément nuls sont premiers entre eux si et seulement si le nombre 1 peut s'écrire comme combinaison linéaire de ces deux nombres.

**A33** On cherche à démontrer une partie du théorème de Bézout.

Soient $a$ et $b$ deux entiers relatifs non simultanément nuls.

On suppose qu'il il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

1. Soit $d \in \mathbb{Z}$ un diviseur commun de $a$ et $b$ : montrer que $d|1$.
2. En déduire que $a$ et $b$ sont premiers entre eux.

*On vient de montrer que : « si 1 peut s'écrire comme combinaison linéaire de $a$ et $b$ alors $a$ et $b$ sont premiers entre eux ».*

*Pour la réciproque voir PDF.*

**A34 Existence d'un inverse modulo $m$**

1. **a.** • 5 admet-il un inverse modulo 7 ?
   • 5 et 7 sont-ils premiers entre eux ?
   **b.** • 6 admet-il un inverse modulo 4 ?
   • 4 et 6 sont-ils premiers entre eux ?

2. On souhaite démontrer que, pour tout $a \in \mathbb{Z}$ et $m \in \mathbb{N}^*$, on a l'équivalence : « $a$ admet un inverse modulo $m$ ⇔ $a$ et $m$ sont premiers entre eux ».

   **a.** On suppose que $a$ admet un inverse modulo $m$.
   Montrer que $a$ et $m$ sont premiers entre eux.

   **b.** On suppose $a$ et $m$ sont premiers entre eux.
   Montrer que $a$ est inversible modulo $m$.

   *On vient bien de démontrer l'équivalence.*

$P$ ▶**Identité de Bézout**

Soient $a$ et $b$ deux entiers relatifs non simultanément nuls.

Il existe $(u, v) \in \mathbb{Z}^2$ tel que :

$$\boldsymbol{au + bv = \text{PGCD}(a, b)}$$

Autrement dit : le PGCD de deux nombres non simultanément nuls peut toujours s'écrire comme combinaison linéaire de ces deux nombres.

**A30 Démontrer la propriété précédente.**

Avec les notations de la propriété, on a :

$$\text{PGCD}(a,b) = \text{PGCD}(a' \times \text{PGCD}(a,b), b' \times \text{PGCD}(a,b))$$
$$= \text{PGCD}(a,b) \times \text{PGCD}(a',b')$$

Résumons : $\text{PGCD}(a,b) = \text{PGCD}(a,b) \times \text{PGCD}(a',b')$.

Or, on a les équivalences :

$$\text{PGCD}(a,b) = \text{PGCD}(a,b) \times \text{PGCD}(a',b')$$
$$\Leftrightarrow \text{PGCD}(a,b) - \text{PGCD}(a,b) \times \text{PGCD}(a',b') = 0$$
$$\Leftrightarrow \text{PGCD}(a,b) \times [1 - \text{PGCD}(a',b')] = 0$$
$$\Leftrightarrow \text{PGCD}(a,b) = 0 \; ou \; 1 - \text{PGCD}(a',b') = 0$$
$$\Leftrightarrow \text{PGCD}(a,b) = 0 \; ou \; \text{PGCD}(a',b') = 1$$

Or, tout PGCD est un entier naturel supérieur ou égal à 1donc $\text{PGCD}(a',b') = 1$ autrement dit $a$ et $b$ sot premiers entre eux.

**A31 Démontrer la propriété précédente.**

Avec les notations de la propriété, on a :

$$\text{PGCD}(a,b) = \text{PGCD}(a' \times d, b' \times d) = |d| \times \text{PGCD}(a',b')$$

résumons : $\text{PGCD}(a,b) = |d| \times \text{PGCD}(a',b')$ $(*)$. Or,

d'une part $d$ est positif donc $|d| = d$,

d'autre part $a'$ et $b'$ sont premiers entre eux donc $\text{PGCD}(a',b') = 1$.

L'égalité $(*)$ devient : $\text{PGCD}(a,b) = d \times 1 = d$ c'est-à-dire :

$\text{PGCD}(a,b) = d$.

**A32 Déterminer tous les $(a,b)$ d'entiers naturels non nuls tels que :**

$$\begin{cases} a \times b = 150 \\ \text{PGCD}(a,b) = 5 \end{cases}$$

Analyse

Supposons que de tels entiers $a$ et $b$ existent, notons $a'$ et $b'$ les entiers naturels les que :

$$a = a' \times \text{PGCD}(a,b) \text{ et } b = b' \times \text{PGCD}(a,b)$$

On sait que $a'$ et $b'$ sont nécessairement premiers entre eux.

On a : $a = a' \times 5$ et $b = b' \times 5$ donc :

$$a \times b = a' \times 5 \times b' \times 5 = 25a'b'$$

Or, $ab = 150$, donc : $25a'b' = 150$ autrement dit : $a'b' = 6$.

Comme $a'$ et $b'$ sont positifs on en déduit que $(a',b')$ est l'un des couples : (1,6), (2,3), (3,2), (6,1) ce qui donne pour $(a,b)$ :

$(5,30)$ $ou$ $(10,15)$ $ou$ $(15,10)$ $ou$ $(30,5)$.

Synthèse

- $5 \times 30 = 150$ et $\text{PGCD}(5,30) = 5$ donc $(5,30)$ est accepté
- $10 \times 15 = 150$ et $\text{PGCD}(10,15) = 5$ donc $(10,15)$ est accepté
- $15 \times 10 = 150$ et $\text{PGCD}(15,10) = 5$ donc $(15,10)$ est accepté
- $30 \times 5 = 150$ et $\text{PGCD}(30,5) = 5$ donc $(30,5)$ est accepté

Conclusion

Les couples cherchés sont $(\mathbf{5,30})$**,** $(\mathbf{10,15})$**,** $(\mathbf{15,10})$ **et** $(\mathbf{30,5})$.

**A33 On cherche à démontrer une partie du théorème de Bézout.**
**Soient $a$ et $b$ deux entiers relatifs non simultanément nuls.**
**On suppose qu'il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.**

1. **Soit $d \in \mathbb{Z}$ un diviseur commun de $a$ et $b$ : montrer que $d|1$.**
   Il existe $(u_0,v_0) \in \mathbb{Z}^2$ tel que $au_0 + bv_0 = 1$.
   On a : $d|a$ et $d|b$ donc $d$ divise toute combinaison linéaire de $a$ et $b$, en particulier $d|au_0 + bv_0$,
   or : $au_0 + bv_0 = 1$ donc $d|1$, donc : $d = -1$ ou $d = 1$.
2. **En déduire que $a$ et $b$ sont premiers entre eux.**
   On en déduit que le seul diviseur positif de $a$ et $b$ est 1, donc que $\text{PGCD}(a,b) = 1$ i.e. que $a$ et $b$ sont premiers entre eux.

Preuve de la réciproque

■ **Démontrons que : $a$ et $b$ sont premiers entre eux $\Rightarrow \exists (u,v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $au + bv = 1$.**

■ Si $a = 0$ et $b \neq 0$

$\text{PGCD}(a,b) = \text{PGCD}(0,b) = |b|$, or $a$ et $b$ sont premiers entre eux donc $\text{PGCD}(a,b) = 1$, d'où : $|b| = 1$ donc $b = -1$ ou $b = 1$ .

On a alors : $a \times 0 + b \times 1 = 1$ (si $b = 1$) et $a \times 0 + b \times (-1) = 1$ (si $b = -1$), par conséquent il existe $u$ et $v$ tels que $au + bv = 1$. ■

■ Si $a \neq 0$

Lemme

Tout diviseur commun de deux entiers non simultanément nuls divise leur PGCD.

Notons $E$ l'ensemble des entiers strictement positifs pouvant s'écrire comme combinaison linéaire de $a$ et $b$, c'est-à-dire pouvant s'écrire sous la forme : $au + bv$.
Démontrons que : $|a| \in E$.
Deux cas seulement peuvent se produire suivant le signe de $a$ :
• si $a > 0$, alors $|a| = a$, et l'égalité $1 \times a + 0 \times b = |a|$ donc : $|a| \in \mathbb{N}^*$ et $|a|$ peut s'écrire comme combinaison linéaire de $a$ et $b$ donc $|a| \in E$.
• si $a < 0$ alors $|a| = -a$ et l'égalité $(-1) \times a + 0 \times b = -a$ s'écrit aussi $(-1)a + 0b = |a|$ donc $|a| \in \mathbb{N}^*$ et $|a|$ peut s'écrire comme combinaison linéaire de $a$ et $b$ donc $|a| \in E$.
Que l'entier relatif non nul $a$ soit strictement positif ou bien strictement négatif on a montré que $|a| \in E$.
L'ensemble $E$ est non vide (il contient $|a|$) et il ne contient que des entiers supérieurs ou égaux à 1 (par définition) donc il est minoré par 1 par conséquent il contient un plus petit élément $m$ et $m \geqslant 1$. La division euclidienne de $a$ par $m$ s'écrit : $a = qm + r$ avec $0 \leqslant r < m$ donc : $r = a - qm$ $(*)$, or $m \in E$ ($m$ est le plus petit élément) donc il existe $u$ et $v$ tels que $au + bv = m$ et en remplaçant dans $(*)$ on obtient :

$$r = a - q(au + bv) = a - qau - qbv = (1 - qu)a + (-qv)b$$

par conséquent il existe deux entiers relatifs $U$ et $V$ tels que $Ua + Vb = r$ ;
supposons que $r > 0$, alors l'égalité $aU + bV = r$ montre que $r \in E$ et comme de plus $r < m$, le nombre $r$ appartenant à $E$ et comme $r < m$ on en déduit que $m$ n'est pas le plus petit élément de $E$ **ce qui est faux**, par conséquent il faut rejeter la supposition $r > 0$ et on peut affirmer que $r \leqslant 0$ et comme on sait par ailleurs que $r \geqslant 0$ on en déduit $r = 0$, donc l'égalité $a = qm + r$ s'écrit $a = qm$ donc $m|a$.
On montrerait de même que $m|b$, par conséquent l'entier naturel strictement positif $m$ est un diviseur commun de $a$ et $b$ donc, d'après le Lemme il divise $\mathrm{PGCD}(a, b)$, or $a$ et $b$ sont premiers entre eux donc $\mathrm{PGCD}(a, b) = 1$, par conséquent $m|1$, d'où $m = 1$.
On a : $m = 1$ et $m \in E$ donc il existe deux entiers relatifs $u$ et $v$ tels que $au + bv = 1$.

Preuve du Lemme
Pour $a$ et $b$ non simultanément nuls : $d|a$ et $d|b \Rightarrow d|\mathrm{PGCD}(a, b)$.

si $b = 0$, $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a, 0) = |a|$ de $d|a \Rightarrow d|\ abs(a) = \mathrm{PGCD}(a, b)$
On a bien $d|\mathrm{PGCD}(a, b)$.
si $b \neq 0$, la division euclidienne de $a$ par $b$ s'écrit $a = q \times b + r_2$ , on note $r_p$ le dernier reste non nul de l'algorithme d'Euclide. On a : $d|a$ et $d|b$ donc $d$ divise toute combinaison linéaire de $a$ et $b$, et en particulier $a - qb = r_2$.
$d|r_1 = b$ et $d|r_2$ donc $d$ divise toute combinaison linéaire de $r_1$ et $r_2$, en particulier $r_3$ (qui est une combinaison linéaire de $r_1$ et $r_2$).
On montre de proche en proche que $d$ divise le dernier reste non nul $r_p$ qui est égal à $\mathrm{PGCD}(a, b)$.

**A34 Existence d'un inverse modulo $m$**

1. a. **• 5 admet-il un inverse modulo 7 ?**
   $5 \times 3 = 15 \equiv 15 - 2 \times 7 \equiv 1\ [7]$ donc **5 admet un inverse modulo 7**
   **• 5 et 7 sont-ils premiers entre eux ?**
   $\mathrm{PGCD}(5,7) = \mathrm{PGCD}(5,7-5) = \mathrm{PGCD}(5,2)$
   $= \mathrm{PGCD}(5-2\times 2,2) = \mathrm{PGCD}(1,2) = 1$
   On a : $\mathrm{PGCD}(5,7) = 1$ donc **5 et 7 sont premiers entre eux**.

   b. **• 6 admet-il un inverse modulo 4 ?**
   On cherche s'il existe $n \in \mathbb{N}$ tel que $6n \equiv 1\ [4]$.
   Utilisons un tableau de congruence modulo 4

| $n \equiv$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $6n \equiv$ | **0** | $6(1)$ $\equiv$ **2** | $6(2)$ $\equiv 12$ $\equiv$ **0** | $6(3)$ $\equiv 2(3)$ $\equiv 6$ $\equiv$ **2** |

   Par disjonction de cas le tableau de congruence précédent montre qu'il n'existe pas $n \in \mathbb{Z}$ tel que : $6n \equiv 1\ [4]$
   donc **6 n'est pas inversible modulo 4**.

   **• 4 et 6 sont-ils premiers entre eux ?**
   $\mathrm{PGCD}(4,6) = \mathrm{PGCD}(4,6-4) = \mathrm{PGCD}(4,2) = 2$
   $(2|4 \text{ et } 2 > 0)$

2. **On souhaite démontrer que « pour tout $a \in \mathbb{Z}$ et $m \in \mathbb{N}^*$, on a l'équivalence : $a$ admet un inverse modulo $m \Leftrightarrow a$ et $m$ sont premiers entre eux »**

   a. **On suppose que $a$ admet un inverse modulo $m$**
   **Montrer que $a$ et $m$ sont premiers entre eux.**
   $a$ admet un inverse modulo $m$ donc il existe $u \in \mathbb{Z}$
   tel que $a \times u \equiv 1\ [m]$, c'est-à-dire tel qu'il existe $k \in \mathbb{Z}$
   tel que : $au = 1 + km$, ce qui s'écrit aussi : $au - km = 1$
   ou encore $au + mv = 1$ en posant $v = -k$.
   Résumons : il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + mv = 1$
   donc d'après le théorème de Bézout $a$ et $m$ sont premiers entre eux.

   b. **On suppose $a$ et $m$ sont premiers entre eux.**
   **Montrer que $a$ est inversible modulo $m$.**
   $a$ et $m$ sont premiers entre eux donc d'après le théorème de Bézout il existe $(u,v) \in \mathbb{Z}^2$ tel que : $au + mv = 1$.
   En raisonnant modulo $m$, on déduit de cette égalité que : $au + 0v \equiv 1\ [m]$, c'est-à-dire : $au \equiv 1\ [m]$ donc $a$ est inversible modulo $m$.

**A35** Justifier qu'il existe $x \in \mathbb{Z}$ tel que : $30x \equiv 1\ [23]$ puis déterminer une valeur possible d'un tel entier $x$.

**A36** Justifier que deux entiers relatifs consécutifs sont nécessairement premiers entre eux.

$P$ $a$, $b$ et $c$ sont trois entiers relatifs, $a$ et $b$ non simultanément nuls.
On considère l'équation $(E) : ax + by = c$ d'inconnue $(x, y) \in \mathbb{Z}^2$.
On a l'équivalence : l'équation $(E)$ admet au moins un couple solution $\Leftrightarrow$ $c$ est un multiple de $\mathrm{PGCD}(a, b)$.

**A37** Démontrer la propriété précédente.

$P$ Soient $a$ et $b$ deux entiers non simultanément nuls et $d$ un entier relatif. On a l'équivalence :
$d$ est un diviseur commun à $a$ et $b \Leftrightarrow d$ divise $\mathrm{PGCD}(a, b)$.

**A38** On souhaite démontrer la propriété précédente.
Soient $a$ et $b$ sont deux entier relatifs non simultanément nuls et $d$ un entier relatif non nul.

1. Justifier qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que : $au + bv = \mathrm{PGCD}(a, b)$.
2. On suppose que $d$ est un diviseur commun de $a$ et $b$, montrer que $d | \mathrm{PGCD}(a, b)$.
3. On suppose que $d | \mathrm{PGCD}(a, b)$, montrer que $d | a$ et $d | b$.

$P$ ▶**Théorème de Gauss**
Soient $a$, $b$, $c$ des entiers relatifs, alors :
si $a$ divise le produit $bc$ et est premier avec $b$, alors $a$ divise $c$.

Si un entier divise un produit et est premier avec l'un des facteurs, alors il divise l'autre facteur.

**A39** Démontrer le théorème de Gauss.

**A40** Un élève affirme que, « pour tous $a$, $b$, $c$ entiers relatifs, si $a | c$ et $b | c$ alors $ab | c$ ». Trouver un contre-exemple.

$P$ ▶**Corollaire du théorème de Gauss**
Soient $a$, $b$, $c$ des entiers relatifs.
Si $a | c$ et $b | c$ avec $a$ et $b$ premiers entre eux, alors $ab | c$.

Autrement dit : si deux nombres premiers entre eux divisent un entier, alors leur produit aussi.

**A41** Démontrer le corollaire du théorème de Gauss.

**A42** Démontrer que : $\forall a \in \mathbb{Z}, 12 | a^2(a^2 - 1)$.

**A43** $(E) : 11x - 5y = 1$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

1. Deviner une solution particulière $(x_0, y_0)$ de $(E)$.
2. Résoudre $(E)$.

**A44** $(E) : 8x - 3y = 1$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

1. Deviner une solution particulière $(x_0, y_0)$ de $(E)$.
2. Résoudre $(E)$.

**A45 d'après BAC S Antilles-Guyane septembre 2008**
On considère le système $(S) \begin{cases} n \equiv 2\ [3] \\ n \equiv 1\ [5] \end{cases}$ d'inconnue $n \in \mathbb{Z}$.

1. Montrer que $11$ est solution de $(S)$.
2. Montrer que : si $n$ est solution de $(S)$, alors : $n \equiv 11\ [15]$.
3. Déterminer toutes les solutions de $(S)$.

**A46** $(E) : 15x - 37y = 1$ d'inconnue $(x, y) \in \mathbb{Z}^2$

1. En utilisant l'algorithme d'Euclide, montrer que $15$ et $37$ sont premiers entre eux.
2. Déterminer une solution particulière $(x_0, y_0)$ de $(E)$.
3. Déterminer toutes les solutions de $(E)$.

**A35 Justifier qu'il existe $x \in \mathbb{Z}$ tel que : $30x \equiv 1\ [23]$ puis déterminer une valeur possible d'un tel entier $x$.**

• il s'agit de savoir si 30 est inversible modulo 23.

Or,

$$\begin{aligned}&\mathrm{PGCD}(30,23) = \mathrm{PGCD}(30-23,23) = \mathrm{PGCD}(7,23)\\&= \mathrm{PGCD}(7,23-3\times 7) = \mathrm{PGCD}(7,2) = \mathrm{PGCD}(7-3\times 2,2)\\&= \mathrm{PGCD}(1,2) = 1\end{aligned}$$

On a : $\mathrm{PGCD}(30,23) = 1$ donc 30 et 23 sont premiers entre eux : 30 est inversible modulo 23 donc il existe $x \in \mathbb{Z}$ tq : $30x \equiv 1\ [23]$

• On a l'équivalence : $30x \equiv 1\ [23] \Leftrightarrow \exists k \in \mathbb{Z}, 30x = 1 + 23k$.

Or, $30x = 1 + 23k \Leftrightarrow 30x - 23k = 1$

Appliquons l'algorithme d'Euclide :

| | |
|---|---|
| | $a = 30$ |
| | $b = 23$ |
| $30 = 23 \times 1 + 7$ | $r_1 = 7$ |
| $23 = 3 \times 7 + 2$ | $r_2 = 2$ |
| $7 = 3 \times 2 + 1$ | $r_3 = 1$ |
| $2 = 2 \times 1 + 0$ | $r_4 = 0$ |

Remontons à partir de l'avant dernière égalités précédentes :

$7 - 3 \times 2 = 1$

$7 - 3(23 - 3 \times 7) = 1$

$7 - 3 \times 23 + 9 \times 7 = 1$

$10 \times 7 - 3 \times 23 = 1$

$10 \times (30 - 23) - 3 \times 23 = 1$

$10 \times 30 - 10 \times 23 - 3 \times 23 = 1$

$10 \times 30 - 13 \times 23 = 1$

En raisonnant modulo 23 on en déduit :

$$10 \times 30 - 13 \times 0 \equiv 1\ [23]$$

autrement dit : $10 \times 30 \equiv 1\ [23]$ donc : $\boldsymbol{x = 10}$ **convient**.

**A36 Justifier que deux entiers relatifs consécutifs sont nécessairement premiers entre eux.**

En notant $n$ le plus petit des deux entiers consécutifs, le deuxième est $n + 1$.

On a : $\mathrm{PGCD}(n, n+1) = \mathrm{PGCD}(n, n+1-n) = \mathrm{PGCD}(n,1) = 1$.

Résumons : $\mathrm{PGCD}(n, n+1) = 1$ donc $n$ et $n+1$ sont premiers entre eux.

$P$ $a$, $b$ et $c$ sont trois entiers relatifs, $a$ et $b$ non simultanément nuls.
On considère l'équation $(E)$ : $ax + by = c$ d'inconnue $(x, y) \in \mathbb{Z}^2$.
On a l'équivalence : l'équation $(E)$ admet au moins un couple solution $\Leftrightarrow$ $c$ est un multiple de $\mathrm{PGCD}(a, b)$.

**A37 Démontrer la propriété précédente.**

**• supposons que $c$ soit un multiple de $\mathrm{PGCD}(a, b)$ et montrons que $(E)$ admet au moins une solution**

$c$ est un multiple de $\mathrm{PGCD}(a, b)$ donc il existe $k \in \mathbb{Z}$ tel que $c = k \times \mathrm{PGCD}(a, b)$.

Or, d'après l'identité de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que :

$$au + bv = \mathrm{PGCD}(a, b)$$

En multipliant chaque membre par $k$, on obtient :

$$\begin{aligned}&k \times (au + bv) = k \times \mathrm{PGCD}(a, b)\\&\Leftrightarrow a \times ku + b \times kv = c\end{aligned}$$

Donc $\exists (x, y) \in \mathbb{Z}^2$ tel que $ax + by = c$, à savoir $(x, y) = (ku, kv)$.

**• supposons que $(E)$ admet au moins un couple solution et montrons que $c$ est un multiple de $\mathrm{PGCD}(a, b)$**

Par hypothèse, $\exists (x_0, y_0) \in \mathbb{Z}^2$ tel que : $ax_0 + by_0 = c$.

$\mathrm{PGCD}(a, b) | a$ et $\mathrm{PGCD}(a, b) | b$ donc $\mathrm{PGCD}(a, b)$ divise toute combinaison linéaire entre $a$ et $b$, en particulier :

$$\mathrm{PGCD}(a, b) | ax_0 + by_0$$

Or, $ax_0 + by_0 = c$, donc $\mathrm{PGCD}(a, b) | c$ autrement dit $c$ est un multiple de $\mathrm{PGCD}(a, b)$.

$P$ Soient $a$ et $b$ deux entiers non simultanément nuls et $d$ un entier relatif. On a l'équivalence :
$d$ est un diviseur commun à $a$ et $b \Leftrightarrow d$ divise $\text{PGCD}(a,b)$.

**A38 On souhaite démontrer la propriété précédente.**
**$a$ et $b$ sont deux entier relatifs et $d$ un entier relatif non nul.**

1. **Justifier qu'il existe $(u,v) \in \mathbb{Z}^2$ tel que $au+bv = \text{PGCD}(a,b)$.**
   D'après l'identité de Bézout il existe $(u,v) \in \mathbb{Z}^2$ tel que :
   $$au+bv = \text{PGCD}(a,b)\ (*)$$
2. **On suppose que $d$ est un diviseur commun de $a$ et $b$.**
   **Montrons que : $d|\text{PGCD}(a,b)$.**
   On suppose que $d$ est un diviseur commun de $a$ et $b$.
   On a : $d|a$ et $d|b$ donc $d$ divise toute combinaison linéaire de $a$ et $b$, en particulier : $d|au+bv$, autrement dit : $d|\text{PGCD}(a,b)$.
3. **On suppose que $d|\text{PGCD}(a,b)$, montrons que $d|a$ et $d|b$.**
   On a : $d|\text{PGCD}(a,b)$.
   Or, $\text{PGCD}(a,b)|a$, donc par transitivité : $d|a$.
   De même, $d|\text{PGCD}(a,b)$ et $\text{PGCD}(a,b)|b$ donc $d|b$.
   Conclusion : $d$ est un diviseur commun de $a$ et $b$.

$P$ ▶**Théorème de Gauss**
Soient $a$, $b$, $c$ des entiers relatifs.
Si $a$ divise le produit $bc$ et est premier avec $b$, alors $a$ divise $c$.

Autrement dit : si un entier divise un produit et est premier avec l'un des facteurs, alors il divise l'autre facteur.

**A39 Démontrer le théorème de Gauss.**
**Soient $a$, $b$, $c$ des entiers relatifs tels que $a|bc$ avec $a$ et $b$ premiers entre eux, montrons que $a|c$.**
On a : $a$ et $b$ premiers entre eux donc d'après le théorème de Bézout il existe $(u,v) \in \mathbb{Z}^2$ tel que : $au+bv = 1$.
Multiplions par $c$ chaque membre, on obtient : $c(au+bv) = c \times 1$
ou encore : $cu \times a + v \times bc = c$. Or, $a|a$ et $a|bc$ (par hypothèse)
donc $a$ divise toute combinaison linéaire de $a$ et $bc$, en particulier $a|cu \times a + v \times bc$ c'est-à-dire : $a|c$.

**A40 Un élève affirme que, « pour tous $a$, $b$, $c$ entiers relatifs, si $a|c$ et $b|c$ alors $ab|c$ ». Trouver un contre-exemple.**
On a $4|12$ et $6|12$ mais non$(4 \times 6|12)$.

$P$ ▶**Corollaire du théorème de Gauss**
Soient $a$, $b$, $c$ des entiers relatifs.
Si $a|c$ et $b|c$ avec $a$ et $b$ premiers entre eux, alors $ab|c$.

Autrement dit : « si deux nombres premiers entre eux divisent un entier, alors leur produit aussi ».

**A41 Démontrer le corollaire du théorème de Gauss.**
**Soient $a$, $b$, $c$ des entiers relatifs tels que : $a|c$ et $b|c$ avec $a$ et $b$ premiers entre eux,montron que $ab|c$.**
On a : $a|c$ donc $\exists k \in \mathbb{Z}, c = ka$ et $b|c$ donc $\exists k' \in \mathbb{Z}, c = k'b\ (*)$.
Les deux écritures de $c$ obtenues impliquent : $ka = k'b$.
On a : $a|ka$ et $ka = k'b$ donc $a|k'b$.
On a : $a|k'b$ avec $a$ et $b$ premiers entre eux, donc d'après le théorème de Gauss on en déduit $a|k'$ : il existe $k'' \in \mathbb{Z}, k' = k''a$.
Remplaçons dans $(*)$ : $c = k''a \times b$.
On a : $c = k'' \times ab$ donc : $ab|c$.

**A42 Démontrer que : $\forall a \in \mathbb{Z}, 12|a^2(a^2-1)$.**
$12 = 3 \times 4$ avec $\text{PGCD}(3,4) = \text{PGCD}(3,4-3) = \text{PGCD}(3,1) = 1$
donc 3 et 4 sont premiers entre eux.
Soit $a$ un entier relatif.
• **montrons que : $3|a^2(a^2-1)$**
Utilisons un tableau de congruence **modulo 3**

| $a \equiv$ | 0 | 1 | 2 |
|---|---|---|---|
| $a^2(a^2-1) \equiv$ | $0^2(0^2-1)$ $\equiv 0$ | $1^2(1^2-1)$ $\equiv 1 \times 0$ $\equiv 0$ | $2^2(2^2-1)$ $\equiv 4 \times 3$ $\equiv 0$ |

Donc par disjonction de cas : $\forall a \in \mathbb{Z}, a^2(a^2-1) \equiv 0\ [3]$
autrement dit : $\forall a \in \mathbb{Z}, 3|a^2(a^2-1)$.

• **montrons que : $4|a^2(a^2-1)$**
Utilisons un tableau de congruence **modulo 4**

| $n \equiv$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $n^2(n^2-1) \equiv$ | $0^2(0^2-1)$ $\equiv 0$ | $1^2(1^2-1)$ $\equiv 1\times 0$ $\equiv 0$ | $2^2(2^2-1)$ $\equiv 4(4-1)$ $\equiv 4\times 3$ $\equiv 0$ | $3^2(3^2-1)$ $\equiv 9\times 8$ $\equiv 1\times 0$ $\equiv 0$ |

Donc par disjonction de cas : $\forall a \in \mathbb{Z}, a^2(a^2-1) \equiv 0\ [4]$
autrement dit : $\forall a \in \mathbb{Z}, 4|a^2(a^2-1)$.

• soit $a \in \mathbb{Z}$, on a : $3|a^2(a^2-1)$ et $4|a^2(a^2-1)$ avec 3 et 4 premiers entre eux donc d'après le corollaire du théorème de Gauss on en déduit : $3\times 4|a^2(a^2-1)$ c'est-à-dire : $12|a^2(a^2-1)$.

Conclusion : $\forall \boldsymbol{a \in \mathbb{Z}, 12|a^2(a^2-1)}$.

**A43** $\boldsymbol{(E): 11x-5y=1, (x,y)\in\mathbb{Z}^2}$

1. **Deviner une solution particulière $(x_0, y_0)$ de $(E)$.**
   On remarque que : $11\times 1-5\times 2=1$ donc $(x_0,y_0)=(1,2)$ est une solution particulière de $(E): 11x-5y=1$.

2. **Résoudre $(E)$.**
   Analyse
   $(x,y)$ est un couple solution de $(E) \Leftrightarrow 11x-5y=1$, et comme $11x_0-5y_0=1$ on obtient :
   $11x-5y=11x_0-5y_0 \Leftrightarrow 11x-11x_0=5y-5y_0$
   $\Leftrightarrow 11(x-x_0)=5(y-y_0)\ (*)$.
   On a : $11|11(x-x_0)$ et $11(x-x_0)=5(y-y_0)$
   donc $11|5(y-y_0)$.
   $\mathrm{PGCD}(11,5)=\mathrm{PGCD}(11-2\times 5,5)=\mathrm{PGCD}(1,5)=1$
   donc 11 et 5 sont premiers entr eux.
   On a : $11|5(y-y_0)$ avec 11 et 5 premiers entre eux donc d'après le théorème de Gauss on en déduit : $11|y-y_0$, par conséquent il existe $k\in\mathbb{Z}, y-y_0=11k$ autrement dit tel que : $y=y_0+11k$.
   Remplaçons dans $(*)$ :
   $11(x-x_0)=5\times 11k \Leftrightarrow x-x_0=5k \Leftrightarrow x=x_0+5k$
   Les couples solution de $(E)$ sont de la forme $(x_0+5k, y_0+11k)$, $k\in\mathbb{Z}$.

   Synthèse
   Considérons un couple $(x_0+5k, y_0+11k)$ où $k\in\mathbb{Z}$.
   On a :
   $11(x_0+5k)-5(y_0+11k)$
   $=11x_0+55k-5y_0-55k$
   $=11x_0-5y_0$
   $=1$ , $(x_0,y_0)$ étant une solution de $(E)$
   donc $(x_0+5k, y_0+11k)$ est solution de $(E)$.

   Conclusion
   Les solutions de $(E)$ sont les couples $(x_0+5k, y_0+11k)$, $k\in\mathbb{Z}$, c'est-à-dire : $\boldsymbol{(1+5k, 2+11k)}$ **où** $\boldsymbol{k\in\mathbb{Z}}$.

**A44** $\boldsymbol{(E): 8x-3y=1}$ **d'inconnue** $\boldsymbol{(x,y)\in\mathbb{Z}^2}$.

1. **Deviner une solution particulière $(x_0, y_0)$ de $(E)$.**
   On a : $8\times 2-3\times 5=16-15=1$ donc $(x_0,y_0)=(2,5)$ est une solution particulière de $(E)$.

2. **Résoudre $(E)$.**
   Analyse
   $(x,y)$ est un couple solution de $(E) \Leftrightarrow 8x-3y=1$, et comme $8x_0-3y_0=1$ on obtient :
   $8x-3y=8x_0-3y_0 \Leftrightarrow 8x-8x_0=3y-3y_0$
   $\Leftrightarrow 8(x-x_0)=3(y-y_0)(*)$
   On a : $8|8(x-x_0)$ et $8(x-x_0)=3(y-y_0)$ donc $8|3(y-y_0)$.
   $\mathrm{PGCD}(8,3)=\mathrm{PGCD}(8-3(3),3)=\mathrm{PGCD}(-1,3)=\mathrm{PGCD}(1,3)$
   $=1$donc 8 et 3 sont premiers entre eux.

On a : $8|3(y-y_0)$ avec 8 et 3 premiers entre eux donc d'après le théorème de Gauss on en déduit $8|y-y_0$ : il existe $k \in \mathbb{Z}$ tel que $y-y_0=8k$ autrement dit tel que : $y=y_0+8k$.
Remplaçons dans $(*)$ :
$8(x-x_0)=3\times 8k \Leftrightarrow x-x_0=3k \Leftrightarrow x=x_0+3k$.
Les couples solution de $(E)$ sont tous de la forme $(x_0+3k, y_0+8k)$, $k \in \mathbb{Z}$.

Synthèse
Considérons un couple $(x_0+3k, y_0+8k)$ où $k \in \mathbb{Z}$, on a :
$8(x_0+3k)-3(y_0+8k)$
$=8x_0+24k-3y_0-24k$
$=8x_0-3y_0$
$=1$, $(x_0, y_0)$ étant un couple solution de $(E)$.
donc $(x_0+3k, y_0+8k)$ est solution de $(E)$.

Conclusion
Les solutions de $(E)$ sont les couples $(x_0+3k, y_0+8k)$, $k \in \mathbb{Z}$, c'est-à-dire : $\boldsymbol{(2+3k, 5+8k)}$ **où** $\boldsymbol{k \in \mathbb{Z}}$**.**

**A45** $\boldsymbol{n \in \mathbb{Z}}$

$$(\boldsymbol{S})\begin{cases}\boldsymbol{n \equiv 2\ [3]}\\ \boldsymbol{n \equiv 1\ [5]}\end{cases}$$

1. **Montrons que 11 est solution de $(S)$.**
• raisonnons modulo 3 :
$11 \equiv 11-3\times 3 \equiv 2\ [3]$ donc 11 vérifie la première ligne du système $(S)$
• raisonnons modulo 5 :
$11 \equiv 11-2\times 5 \equiv 1\ [5]$ donc 11 vérifie la deuxième ligne du système $(S)$

Il résulte des deux points précédents que 11 est solution de $(S)$.

2. **Montrons que : si $n$ est solution de $(S)$ alors $n \equiv 11\ [15]$.**
Remarquons d'abord que :
$\mathrm{PGCD}(3,5)=\mathrm{PGCD}(3,5-3)=\mathrm{PGCD}(3,2)=\mathrm{PGCD}(3-2,2)$
$=\mathrm{PGCD}(1,2)=1$ donc 3 et 5 sont premiers entre eux.

Soit $n$ une solution de $(S)$, on a : $n \equiv 2\ [3]$ et $n \equiv 1\ [5]$.
• $n \equiv 2\ [3]$
donc : $n-11 \equiv 2-11 \equiv -9 \equiv -9+3\times 3 \equiv 0\ [3]$
On a : $n-11 \equiv 0\ [3]$ donc $3|n-11$

• $n \equiv 1\ [5]$
donc : $n-11 \equiv 1-11 \equiv -10 \equiv -10+2\times 5 \equiv 0\ [5]$
$n-11 \equiv 0\ [5] \Leftrightarrow 5|n-11$

On a : $3|n-11$ et $5|n-11$ avec 3 et 5 **premiers entre eux** donc d'après le corollaire du théorème de Gauss on en déduit que $3\times 5|n-11$, c'est-à-dire $15|n-11$, ou encore : $\boldsymbol{n \equiv 11\ [15]}$.

3. Analyse
Si $n$ est solution de $(S)$ alors $n \equiv 11\ [15]$ (question précédente).
Toute solution de $(E)$ est de la forme $n \equiv 11\ [15]$.

Synthèse
Soit $n$ tel que $n \equiv 11\ [15]$ : il existe $k \in \mathbb{Z}$, $n=11+15k$.
On a alors :
• $n=11+15k \equiv 11+15k-5k\times 3 \equiv 11-3(3) \equiv 2\ [3]$
$n \equiv 2\ [3]$ donc $n$ vérifie la première ligne du système $(S)$
• $n=11+15k \equiv 11+15k-3k\times 5 \equiv 11-2\times 5 \equiv 1\ [5]$
$n \equiv 1\ [5]$ donc $n$ vérifie la première ligne du système $(S)$

Il résulte des deux points précédents que $n$ est solution du système $(S)$.

Conclusion
**Les solutions de $(S)$ sont les entiers relatifs $n$ tels que :**
$\boldsymbol{n \equiv 11\ [15]}$**.**

**A46** $(x, y) \in \mathbb{Z}^2 : 15x - 37y = 1$ $(E)$

**1.** En appliquant l'algorithme d'Euclide, on obtient :

| | |
|---|---|
| | $a = 37$ |
| | $b = 15$ |
| $37 = 2 \times 15 + \mathbf{7}$ | $r_1 = 7$ |
| $15 = 2 \times 7 + \mathbf{1}$ | $r_2 = 1$ |
| $7 = 7 \times 1 + \mathbf{0}$ | $r_3 = 0$ |

Le PGCD est le dernier reste non nul donc $\text{PGCD}(15, 37) = 1$ : les nombres 15 et 37 sont premiers entre eux.

**2.** En remontant les calculs précédents à partir de l'avant dernière ligne :

$15 - 2 \times 7 = 1$

$15 - 2 \times (37 - 2 \times 15) = 1$

$15 - 2 \times 37 + 4 \times 15 = 1$

$5 \times 15 - 2 \times 37 = 1$

On a donc : $15 \times x_0 - 37 \times y_0 = 1$ donc $(x_0, y_0) = (5, 2)$ est une solution particulière de $(E) : 15x - 37y = 1$.

**3.** Analyse

Soit $(x, y)$ un couple solution de $(E)$, on a : $15x - 37y = 1$.

Or $(x_0, y_0)$ est solution de $(E)$ donc : $1 = 15x_0 - 37y_0$, d'où :

$15x - 37y = 15x_0 - 37y_0 \Leftrightarrow 15(x - x_0) = 37(y - y_0)$ $(*)$.

$15|15(x - x_0)$ et $15(x - x_0) = 37(y - y_0)$ donc $15|37(y - y_0)$

On a : $15|37(y - y_0)$ avec 15 et 37 premiers entre eux donc d'après le théorème de Gauss on en déduit $15|y - y_0$ : il existe $k \in \mathbb{Z}, y - y_0 = 15k$ autrement dit : $y = y_0 + 15k$.

Remplaçons dans $(*)$ :

$15(x - x_0) = 37 \times 15k \Leftrightarrow x - x_0 = 37k \Leftrightarrow x = x_0 + 37k$

Les couples solutions de $(E)$ sont tous de la forme $(x_0 + 37k, y_0 + 15k)$, $k \in \mathbb{Z}$.

Synthèse

Considérons un couple $(x_0 + 37k, y_0 + 15k)$ où $k \in \mathbb{Z}$.

On a :

$15(x_0 + 37k) - 37(y_0 + 15k)$

$= 15x_0 + 15 \times 37k - 37y_0 - 37 \times 15k$

$= 15x_0 - 37y_0$

$= 1$ , $(x_0, y_0)$ est une solution de $(E)$.

Résumons : $15(x_0 + 37k) - 37(y_0 + 15k) = 1$

donc $(x_0 + 37k, y_0 + 15k)$ est solution de $(E)$.

Conclusion

Les solutions de $(E)$ sont les couples $(x_0 + 37k, y_0 + 15k)$, $k \in \mathbb{Z}$, c'est-à-dire les couples : $(\mathbf{5 + 37k, 2 + 15k})$ **où** $\boldsymbol{k} \in \mathbb{Z}$.

**A47** On considère le système d'inconnue $n \in \mathbb{Z}$ :

$$(S)\begin{cases} n \equiv 2\ [3] \\ n \equiv 6\ [7] \end{cases}$$

1. Montrer que $20$ est solution de $(S)$.
2. Montrer que : si $n$ est solution de $(S)$, alors : $n \equiv 20\ [21]$.
3. Déterminer toutes les solutions de $(S)$.

**A48 D'après bac Antilles-Guyane Juin 2011**

*Les questions* **1.** *et* **2.** *sont indépendantes.*

1. On considère l'équation $(E)$ : $11x - 7y = 5$ où $x$ et $y$ sont des entiers relatifs.
   - **a.** Trouver un couple $(u_0, v_0) \in \mathbb{Z}^2$ tel que : $11u_0 - 7v_0 = 1$.
     En déduire une solution particulière $(x_0, y_0)$ de $(E)$.
   - **b.** Résoudre $(E)$.
   - **c.** Dans le plan munit d'un repère orthogonal on considère la droite $\mathcal{D}$ d'équation : $11x - 7y - 5 = 0$.
     Déterminer les points $M(x; y)$ de $\mathcal{D}$ à coordonnées entières tels que : $0 \leqslant x \leqslant 50$ et $0 \leqslant y \leqslant 50$.
2. On considère l'équation $(F)$: $11x^2 - 7y^2 = 5$ où $x$ et $y$ sont des entiers relatifs.
   - **a.** Démontrer que :
     si $(x, y)$ est solution de $(F)$, alors $x^2 \equiv 2y^2\ [5]$.
   - **b.** Donner le tableau de congruence de $x^2$ modulo $5$ et celui de $2y^2$ modulo $5$.
   - **c.** En déduire que :
     si $(x, y)$ est solution de $(F)$, alors $x$ et $y$ sont divisibles par $5$.
   - **d.** Démontrer que : si $x$ et $y$ sont divisibles par $5$, alors $(x, y)$ n'est pas solution de $(F)$.
     Que peut-on en déduire pour l'équation $(F)$ ?

**A49** On note $(E)$ l'équation d'inconnue $(u, v) \in \mathbb{Z}^2$ : $12u + 5v = 2$.

- trouver une solution particulière $(u_0, v_0)$ de $(E)$
- déterminer toutes les solutions de $(E)$

**A50** Démontrer que, pour tout $m \in \mathbb{Z}$, $14 | m^7 - m$.

**A51** Après une rude bataille, le général Wu doit ramener ses hommes au camp de base :
s'il forme des groupes de 16 alors $10$ de ses hommes restent à l'écart, et s'il forme des groupes de $25$ alors $6$ de ses hommes restent à l'écart.
Combien d'hommes reste-t-il au général Wu sachant que ce nombre est situé entre $700$ et $1\,000$ ?

**A47** $n \in \mathbb{Z}$

$$(S)\begin{cases} n \equiv 2\ [3] \\ n \equiv 6\ [7] \end{cases}$$

1. **Montrons que 20 est solution de $(S)$.**
   • raisonnons modulo 3 :
   $20 \equiv 20 - 6 \times 3 \equiv 2\ [3]$ donc 20 vérifie la première ligne du système $(S)$
   • raisonnons modulo 7:
   $20 \equiv 20 - 2 \times 7 \equiv 6\ [7]$ donc 20 vérifie la deuxième ligne du système $(S)$
   Il résulte des deux points précédents que 20 est solution de $(S)$.

2. **Montrons que : si $n$ est solution de $(S)$, alors : $n \equiv 20\ [21]$.**
   Soit $n$ une solution de $(S)$ donc $n \equiv 2\ [3]$ et $n \equiv 6\ [7]$.
   Remarquons d'abord que :
   $\text{PGCD}(3,7) = \text{PGCD}(3, 7 - 2 \times 3) = \text{PGCD}(3,1) = 1$ donc 3 et 7 sont premiers entre eux.

   Soit $n$ une solution de $(S)$, on a : $n \equiv 2\ [3]$ et $n \equiv 6\ [7]$.
   • $n \equiv 2\ [3]$
   donc : $n - 20 \equiv 2 - 20 \equiv -18 \equiv -18 + 6 \times 3 \equiv 0\ [3]$
   On a : $n - 20 \equiv 0\ [3]$ donc $3|n - 20$

   • $n \equiv 6\ [7]$
   donc : $n - 20 \equiv 6 - 20 \equiv -14 \equiv -14 + 2 \times 7 \equiv 0\ [7]$
   $n - 20 \equiv 0\ [7]$ donc $7|n - 20$

   On a : $3|n - 20$ et $7|n - 20$ avec 3 et 7 **premiers entre eux** donc d'après le corollaire du théorème de Gauss on en déduit que $3 \times 7|n - 20$, c'est-à-dire $21|n - 20$, ou encore : $\boldsymbol{n \equiv 20\ [21]}$.

3. Déterminons toutes les solutions de $(S)$.
   <u>Analyse</u>
   Si $n$ est solution de $(S)$ alors $n \equiv 20\ [21]$ (question précédente).
   Toute solution de $(E)$ est donc de la forme $n \equiv 20\ [21]$.

<u>Synthèse</u>
Soit $n \in \mathbb{Z}$ tel que $n \equiv 20\ [21]$ : il existe $k \in \mathbb{Z}, n = 20 + 21k$.

On a :
• $n - 2 = 20 + 21k - 2 = 18 - 21k = 3(6 - 7k) \equiv 0\ [3]$.
On a : $n - 2 \equiv 0\ [3]$ autrement dit : $n \equiv 2\ [3]$, donc $n$ vérifie la première ligne du système $(S)$.

• $n - 6 = 20 + 21k - 6 = 14 - 21k = 7(2 - 3k) \equiv 0\ [7]$.
On a : $n - 6 \equiv 0\ [7]$ autrement dit : $n \equiv 6\ [7]$, donc $n$ vérifie la deuxième ligne du système $(S)$.

Il résulte des deux points précédents que $n$ est solution de $(S)$.

<u>Conclusion</u>
**Les solutions de $(S)$ sont les entiers relatifs $n$ tels que :**
$\boldsymbol{n \equiv 20\ [21]}$.

**A48 D'après bac Antilles-Guyane Juin 2011**

**1.** $(E)$ : $11x - 7y = 5$, $x$ et $y$ entiers relatifs

**a. Trouver un couple $(u_0, v_0) \in \mathbb{Z}^2$ tel que : $11u_0 - 7v_0 = 1$.**

On a : $11 \times 2 - 7 \times 3 = 22 - 21 = 1$ donc : $(u_0, v_0) = (2, 3)$ convient.

On a : $11 \times 2 - 7 \times 3 = 1$, donc en multipliant chaque membre par 5 : $11 \times 10 - 7 \times 15 = 5$ par conséquent $(10,15)$ est une solution particlière de $(E)$.

Conclusion : $(x_0, y_0) = (10, 15)$ convient.

**b. Résoudre $(E)$.**

(non rédigé) Les solutions de $(E)$ sont les couples $(10 + 7k, 15 + 11k)$, $k \in \mathbb{Z}$.

**c. $\mathcal{D}$ d'équation : $11x - 7y - 5 = 0$, déterminer les points $M(x; y)$ de $\mathcal{D}$ à coordonnées entières tels que : $0 \leqslant x \leqslant 50$ et $0 \leqslant y \leqslant 50$.**

Soit $(x; y)$ les coordonnées d'un tel point $M$, on a d'une part : $11x - 7y - 5 = 0$ autrement dit : $11x - 7y = 5$ donc d'après **1.b.** il existe $k \in \mathbb{Z}$ tel que : $(x, y) = (10 + 7k, 15 + 11k)$, d'autre part, $0 \leqslant x \leqslant 50$ et $0 \leqslant y \leqslant 50$ donc :

$$\begin{cases} 0 \leqslant 10 + 7k \leqslant 50 \\ 0 \leqslant 15 + 11k \leqslant 50 \end{cases} \Leftrightarrow \begin{cases} -10 \leqslant 7k \leqslant 40 \\ -15 \leqslant 11k \leqslant 35 \end{cases}$$

$$\Leftrightarrow \begin{cases} k \in \{-1; 0; 1; 2; 3; 4; 5\} \\ k \in \{-1; 0; 1; 2; 3\} \end{cases} \Leftrightarrow k \in \{-1; 0; 1; 2; 3\}$$

On obtient finalement les cinq points :

$A(3; 4)$, $B(10; 15)$, $C(17; 26)$, $D(24; 37)$ et $E(31; 48)$.

**2.** $(F)$: $11x^2 - 7y^2 = 5$ où $x$ et $y$ sont des entiers relatifs

**a. Démontrer que :**

**si $(x, y)$ est solution de $(F)$, alors $x^2 \equiv 2y^2$ [5].**

Supposons que : $11x^2 - 7y^2 = 5$.

Raisonnons modulo 5.

$11 \equiv 11 - 2 \times 5 \equiv 1$ [5], $7 \equiv 7 - 1 \times 5 \equiv 2$ [5] et $5 \equiv 0$ [5], donc l'égalité : $11x^2 - 7y^2 = 5$ implique : $1x^2 - 2y^2 \equiv 0$ [5], qui s'écrit aussi :

$x^2 - 2y^2 + 2y^2 \equiv 0 + 2y^2$ [5] ou encore : $x^2 \equiv 2\,y^2$ [5].

**b. Donner le tableau de congruence de $x^2$ modulo 5 et celui de $2y^2$ modulo 5.**

• tableau de congruence modulo 5

| $x \equiv$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $x^2 \equiv$ | 0 | 1 | 4 | $9 \equiv 4$ | $16 \equiv 1$ |

• tableau de congruence modulo 5

| $y \equiv$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $2x^2 \equiv$ | 0 | 2 | $8 \equiv 3$ | $18 \equiv 3$ | $32 \equiv 2$ |

**c. En déduire que :**

**si $(x, y)$ est solution de $(F)$, alors $x$ et $y$ sont divisibles par 5.**

Si $(x, y)$ est solution de $(F)$ alors $x^2 \equiv 2y^2$ [5] (question **a.**), or cela ne se produit que pour $x^2 \equiv 2y^2 \equiv 0$ [5] et on a alors par lecture inverse des tableaux de congruences :

$x \equiv 0$ [5] et $y \equiv 0$ [5], c'est-à-dire : $5|x$ et $5|y$.

**d. Démontrer que : si $x$ et $y$ sont divisibles par 5, alors $(x, y)$ n'est pas solution de $(F)$.**

Supposons $x$ et $y$ divisibles par 5 : il existe $k \in \mathbb{Z}$ et il existe $k' \in \mathbb{Z}$ tels que $x = 5k$ et $y = 5k'$. Or, $(x, y)$ est solution de $(F)$ : $11x^2 - 7y^2 = 5$ donc : $11(5k)^2 - 7(5k')^2 = 5$, c'est-à-dire : $11 \times 25k^2 - 7 \times 25\,k'^2 = 5$ autrement dit : $25(11k^2 - 7k'^2) = 5$. On a : $25|25(11k^2 - 7k'^2)$ et $25(11k^2 - 7k'^2) = 5$ donc : $25|5$ ce qui est FAUX, par conséquent il faut rejeter la supposition d'existence d'une solution à l'équation $(F)$.

**On en déduit que $(F)$ n'admet pas de solution.**

**A49** $(E)$ **d'inconnue** $(u, v) \in \mathbb{Z}^2$ **:** $12u + 5v = 2$

• **solution particulière** $(u_0, v_0)$ **de** $(E)$

On a : $12 \times 1 + 5 \times (-2) = 12 - 10 = 2$ donc $(u_0, v_0) = (1, -2)$ est une couple solution.

• **résolution de** $(E)$

Analyse

$\text{PGCD}(12,5) = \text{PGCD}(12 - 2(5), 5) = \text{PGCD}(2,5)$
$= \text{PGCD}(2,5 - 2 \times 2) = \text{PGCD}(5,1) = 1$ donc 12 et 5 sont premiers entre eux. Avec les notations de l'exercice, on a les équivalences :

$(u, v)$ est solution de $(E) \Leftrightarrow 12u + 5v = 2$
$\Leftrightarrow 12u + 5v = 12u_0 + 5v_0 \Leftrightarrow 12u - 12u_0 = 5v_0 - 5v$
$\Leftrightarrow 12(u - u_0) = 5(v_0 - v)$ $(*)$

On a : $12|12(u - u_0)$ et $12(u - u_0) = 5(v_0 - v)$ donc $12|(v_0 - v)$.
On a : $12|5(v_0 - v)$ avec 12 et 5 premiers entre eux, donc d'après le théorème de Gauss on en déduit $12|v_0 - v$, autremet dit il existe $k \in \mathbb{Z}$ tel que : $v_0 - v = 12k$, qui s'écrit aussi : $v = v_0 - 12k$.
Remplaçons dans $(*)$ :

$12(u - u_0) = 5 \times 12k \Leftrightarrow u - u_0 = 5k \Leftrightarrow u = u_0 + 5k$

Synthèse

Vérifions que tout couple $(u_0 + 5k, v_0 - 12k)$, $k \in \mathbb{Z}$, est solution de $(E)$ :

$$\begin{aligned} &12(u_0 + 5k) + 5(v_0 - 12k) \\ &= 12u_0 + 12 \times 5k + 5v_0 - 5 \times 12k \\ &= \underbrace{12u_0 + 5v_0}_{2} + \underbrace{60k - 60k}_{0} \\ &= 2 \end{aligned}$$

On a : $12(u_0 + 5k) + 5(v_0 - 12k) = 2$ donc $(u_0 + 5k, v_0 - 12k)$ est un couple solution de $(E)$.

Conclusion

Les solutions de $(E)$ sont les couples $(1 + 5k, -2 - 12k)$, $k \in \mathbb{Z}$.

**A50** **Démontrer que, pour tout** $m \in \mathbb{Z}$, $14|m^7 - m$.

Soit $m \in \mathbb{Z}$.

☐ **montrons que :** $2|m^7 - m$

Utilisons un tableau de congruence modulo 2

| $m \equiv$ | 0 | 1 |
|---|---|---|
| $m^7 - m \equiv$ | $0^7 - 0$ $\equiv 0$ | $1^7 - 1$ $\equiv 1 - 1$ $\equiv 0$ |

Pour tout $m \in \mathbb{Z}, m^7 - m \equiv 0\ [2]$, autrement dit : $2|m^7 - m$.

☐ **montrons que :** $7|m^7 - m$

• si $m \equiv -3\ [7]$, alors :
$m^7 - m \equiv (-3)^7 - (-3) \equiv ((-3)^2)^3(-3) + 3 \equiv 9^3(-3) + 3$
$\equiv 2^3(-3) + 3 \equiv 8(-3) + 3 \equiv 1(-3) + 3 \equiv \mathbf{0}\ \mathbf{[7]}$

• si $m \equiv -2\ [7]$, alors :
$m^7 - m \equiv (-2)^7 - (-2) \equiv ((-2)^3)^2(-2) + 2 \equiv (-8)^2(-2) + 2$
$\equiv (-1)^2(-2) + 2 \equiv 1 \times (-2) + 2 \equiv -2 + 2 \equiv \mathbf{0}\ \mathbf{[7]}$

• si $m \equiv -1\ [7]$, alors : $m^7 - m \equiv (-1)^7 - (-1) \equiv -1 + 1 \equiv \mathbf{0}\ \mathbf{[7]}$

• si $m \equiv 0\ [7]$, alors : $m^7 - m \equiv 0^7 - 0 \equiv \mathbf{0}\ \mathbf{[7]}$

• si $m \equiv 1\ [7]$, alors : $m^7 - m \equiv 1^7 - 1 \equiv 1 - 1 \equiv \mathbf{0}\ \mathbf{[7]}$

• si $m \equiv 2\ [7]$, alors :
$m^7 - m \equiv 2^7 - 2 \equiv (2^3)^2 \times 2 - 2 \equiv 8^2 \times 2 - 2 \equiv 1^2 \times 2 - 2$
$\equiv 2 - 2 \equiv \mathbf{0}\ \mathbf{[7]}$

• si $m \equiv 3\ [7]$, alors :
$m^7 - m \equiv 3^7 - 3 \equiv (3^2)^3 \times 3 - 3 \equiv 9^3 \times 3 - 3 \equiv 2^3 \times 3 - 3$
$\equiv 8 \times 3 - 3 \equiv 1 \times 3 - 3 \equiv \mathbf{0}\ \mathbf{[7]}$

Par disjonction de cas, on en déduit que : $\forall m \in \mathbb{Z}, m^7 - m \equiv 0\ [7]$ autrement dit : $7|m^7 - m$.

☐ **montrons que $14|m^7 - m$**
remarquons d'abord que :
$\text{PGCD}(2,7) = \text{PGCD}(2, 7-3\times 2) = \text{PGCD}(2,1) = 1$ donc 2 et 7 sont premiers entre eux.

On a : $2|m^7 - m$ et $7|m^7 - m$ avec 2 et 7 premiers entre eux donc d'après le corolaire du théorème de Gauss on en déduit que :
$2\times 7|m^7 - m,$ qui s'écrit aussi : $14|m^7 - m$.

Conclusion : $\forall \boldsymbol{m} \in \mathbb{Z}, \boldsymbol{14|m^7 - m}$.

**A51 Après une rude bataille, le général Wu doit ramener ses soldats au camp de base : s'il forme des groupes de 16 soldats alors 10 de ses hommes restent à l'écart, et s'il forme des groupes de 25 soldats alors 6 soldats restent à l'écart. Combien de soldats reste-t-il au général Wu sachant que ce nombre est situé entre 700 et 1000 ?**

Soit $n$ le nombre de soldats du général Wu, d'après les informations de l'énoncé : $n \equiv 10\ [16]$ et $n \equiv 6\ [25]$. Il s'agit de résoudre :
$(S)\begin{cases} n \equiv 10\ [16] \\ n \equiv 6\ \ [25] \end{cases}$, avec de plus $n \in [\![700\,;1\,000]\!]$.
Recherche d'une solution particulière du système $(S)$ :
Méthode 1
On teste des multiple de 16 augmentées de 10 jusqu'à obtenir un multiple de 25 augmentée de 6.
$2\times 16+10 = 42 = 25+17$ ne convient pas
$3\times 16+10 = 58 = 2\times 25+23$ ne contient pas
$4\times 16+10 = 74 = 2\times 25+24$ ne convient pas
$5\times 16+10 = 90 = 3\times 25+15$ ne convient pas
$6\times 16+10 = 106 = 4\times 25+6$ convient
On a donc :
$$106 = 6\times 16+10 \equiv 10\ [16]$$
$$106 = 4\times 25+6 \equiv 6\ [25]$$
par conséquent 106 est une solution particulière de $(S)$.

Méthode 2
$n \equiv 10\ [16]$ donc il existe $u \in \mathbb{Z}, n = 10+16u$.
$n \equiv 6\ [25]$ donc il existe $v \in \mathbb{Z}, n = 6+25v$.
On en déduit : $10+16u = 6+25v$, puis :$16u-25v = -4$
autrement dit : $-16u+25v = 4$.
Comme $-16$ et 25 sont premiers entre eux, le théorème de Bézout affirme l'existence de $(x_0, y_0) \in \mathbb{Z}^2, -16x_0+25y_0 = 1$, que l'on peut obtenir avec l'algorithme d'Euclide, puis en multipliant par 4 : $-16(4x_0)+25(4y_0) = 4$ donc $(u_0, v_0) = (4x_0, 4y_0)$ est une solution particulière de $-16u+25v = 4$, en remplaçant $u$par $u_0$ dans $n = 10+16u$ (ou $v$ par $v_0$ dans $n = 6+25v$) on obtient une solution particulière $n_0$ du système $(S)$.

[Non rédigé] Les solutions s'écrivent : $n \equiv n_0\ [16\times 25]$ c'est-à-dire : $n \equiv 106\ [400]$.

Il existe donc $k \in \mathbb{Z}$ tel que : $n = 106+400k$.
si $k = 1$, alors : $n = 106+400 = 506 \notin [\![700\,;1\,000]\!]$ donc ne convient pas.
si $k = 2$, $n = 106+400\times 2 = 906 \in [\![700\,;1\,000]\!]$ donc convient.
si $k = 3$, alors : $n = 106+400\times 3 = 1\,306 \notin [\![700\,;1\,000]\!]$ donc ne convient pas.

Le général a donc une armée de **906 soldats**.

Un programme Python donne directement le nombre de soldats :

```
1 for n in range(700,1001):
2     if ((n%16==10) and (n%25==6)):
3         print("n=",n)
```

```
Shell
>>> %Run A131.py
n= 906
```