Arithmétique partie II PGCD, Gauss, Bézout

$\boxed{D}$ 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 : $\forall \boldsymbol{x \in E}, \boldsymbol{x \leqslant m}$

• E **est majoré** s'il existe $m \in \mathbb{Z}$ tel que m est majorant de E :
$\exists \boldsymbol{m \in \mathbb{Z}}, \forall \boldsymbol{x \in E}, \boldsymbol{x \leqslant m}$ (💣 m peut ne pas appartenir à 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 :

m est le plus grand élément de E $\Leftrightarrow \begin{cases} \forall \boldsymbol{x \in E}, \boldsymbol{x \leqslant m} \\ \boldsymbol{m \in E} \end{cases}$

Le maximum de E se note parfois $\max \boldsymbol{E}$.

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

$\boxed{D}$ **Quelques définitions**

• 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 qui est noté $\mathrm{PGCD}(a,b)$ ou $\mathrm{PGCD}(a;b)$

• a et b snt les **deux arguments** dans l'écriture $PGCD(a,b)$

$\boxed{P}$ 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 $\mathrm{PGCD}(7,0)$.

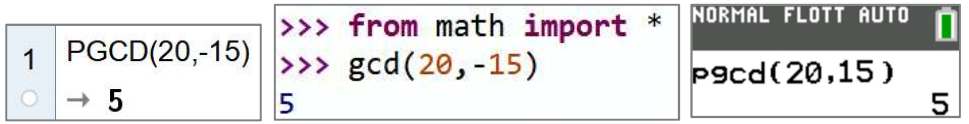
A03 Peut-on définir le $\mathrm{PGCD}(a,b)$ lorsque $a = 0$ et $b = 0$?

$\boxed{P}$ Soient a et b deux entiers relatifs non simultanément nuls, on a :

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

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

$\boxed{i}$ 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** donc dans la recherche du PGCD on pourra donc ne s'intéresser qu'aux listes des diviseurs **positifs**.



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

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

A04 Justifier les deux formules précédentes.

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

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

A06 Justifier la formule précédente.

A07 Déterminer $\mathrm{PGCD}(1,7), \mathrm{PGCD}(0,1), \mathrm{PGCD}(-5,1), \mathrm{PGCD}(1,1)$.

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

[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

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 …
```

[F] Formule de l'addition

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

A14 Démontrer la formule d'addition à partir de la formule de la soustraction.

$\boxed{P}$ a et b appartiennent à $\mathbb{Z}$ et sont non simultanément nuls, $k \in \mathbb{Z}$.

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

(dans un calcul de PGCD on peut ajouter/soustraire à l'un des deux arguments un multiple de l'autre argument)

A15 On se propose de démontrer que, pour a et b entiers relatifs non simultanément nuls et k entier relatif, on a :

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

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. En déduire que : $\forall k \in \mathbb{Z}, \mathrm{PGCD}(a,b) = \mathrm{PGCD}(a, b+ka)$.

A16 Soit $n \in \mathbb{N}$, déterminer :

$$\mathrm{PGCD}(2n+5, n+1) \text{ et } \mathrm{PGCD}(3n+1, n+2)$$

A17 Soit $n \in \mathbb{N}$, déterminer $\mathrm{PGCD}(3n+4, 2n+1)$.

A18 Soit $n \in \mathbb{N}$, déterminer $\mathrm{PGCD}(2n^2 - n - 15, n-3)$.

$\boxed{F}$ **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 :

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

A19 Démontrer la formule du reste.

A20 Déterminer $\mathrm{PGCD}(456, 25)$, $\mathrm{PGCD}(7, 120)$.

$\boxed{P}$ **Algorithme d'Euclide**

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

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

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

si $r_1 = 0$ on s'arrête et :

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

sinon :

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

si $r_2 = 0$ on s'arrête et :

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

donc **$\mathbf{PGCD}(a,b)$ 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 :

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

donc **$\mathbf{PGCD}(a,b)$ 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 :

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

A21 À l'aide de l'algorithme d'Euclide déterminer $\mathrm{PGCD}(108, 40)$.

A22 À l'aide de l'algorithme d'Euclide déterminer $\mathrm{PGCD}(439, 50)$.

$\boxed{D}$ 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 :

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

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

Programme utilisable sur la calculatrice

A23 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** ».

A24 À l'aide de l'algorithme d'Euclide, déterminer $\text{PGCD}(46, 21)$ puis un couple (x_0, y_0) d'entiers relatifs tels que $46x_0 + 21y_0 = 1$.

A25 [calculatrice]
À l'aide de l'algorithme d'Euclide, déterminer $\text{PGCD}(359, 450)$ puis un couple (x_0, y_0) d'entiers relatifs tels que $359x_0 + 450y_0 = 1$.

A26 [calculatrice]
Déterminer $\text{PGCD}(731, 272)$.
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 :

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

A27 Démonstration de la propriété précédente en PDF.

A28 Déterminer $\text{PGCD}(300{,}700)$, $\text{PGCD}(2^{50}, 2^{51})$.

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.

A29 Démontrer la propriété précédente.

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

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

alors d est le PGCD de a et b.

A30 Démontrer la propriété précédente.

A31 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 : $\boldsymbol{au + bv = 1}$

(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)

A32 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.

Pour la réciproque voir PDF.

A33 **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 $m \Leftrightarrow a$ 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.
   b. On suppose a et m sont premiers entre eux.
   Montrer que a est inversible modulo m.

A34 Justifier qu'il existe $x \in \mathbb{Z}$ tel que : $30x \equiv 1\ [23]$ puis déterminer une valeur possible d'un tel entier x.

A35 Justifier que deux entiers relatifs consécutifs sont nécessairement premiers entre eux.

P **Identité de Bézout**
Soient a et b deux entiers relatifs non simultanément nuls,
il existe $(u, v) \in \mathbb{Z}^2$ tel que :

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

(le PGCD de deux nombres non simultanément nuls peut s'écrire comme combinaison linéaire de ces deux nombres)

A36 Démontrer l'identité de Bézout.

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**
a, b, c sont des entiers relatifs,
si a divise bc avec a et b premier entre eux, 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 « 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 $(x, y) \in \mathbb{Z}^2$.

Deviner une solution particulière (x_0, y_0) de (E), puis résoudre (E).

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

Deviner une solution particulière (x_0, y_0) de (E), puis 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).

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 $\in \mathbb{Z}$, $14 | m^7 - m$.

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 ?