Chapitre VII

PGCD-PPMC-BEZOUT-GAUSS

Recherche

Exercice 1 : On dispose d'une surface rectangulaire de papier peint mesurant 630 cm par 600 cm.
On veut découper cette surface en carrés tous identiques, dont le côté mesure un nombre entier de centimètres.

Quelle est la longueur du côté des plus grands carrés que l'on pourra découper ?

Exercice 2 : Un fleuriste dispose de 165 marguerites et de 132 tulipes. Avec ces fleurs, il veut composer des bouquets identiques.

Quel est le plus grand nombre de bouquets qu'il pourra réaliser ?
Quelle sera alors la composition d'un bouquet ?

1. Définition et premières propriétés

Définition 1

Soient a et b deux entiers relatifs non nuls.
On note $D_{\mathbb{Z}}(a,b)$ l'ensemble des diviseurs communs de a et b.

Cet ensemble des diviseurs communs à a et b admet un plus grand élément.
On l'appelle **le plus grand diviseur commun (PGCD)** à a et b, et on le note : $\text{PGCD}(a;b)$.

En guise d'explications

$D_{\mathbb{Z}}(a,b)$, l'ensemble des diviseurs communs de a et b, **n'est pas vide**, puisque 1 divise forcément a et b.
De plus, tous les diviseurs communs à a et b sont inférieurs à $|a|$ et $|b|$.
C'est pour cette raison qu'on peut affirmer que $D_{\mathbb{Z}}(a,b)$ possède un plus grand élément, le PGCD de a et b, et que ce PGCD est forcément positif (car supérieur à 1).

Recherche

Exercice 3 : Déterminer $\text{PGCD}(105;45)$, en dressant la liste des diviseurs de chacun de ces entiers.

Propriété 1

- $\text{PGCD}(a;b) = \text{PGCD}(|a|;|b|)$
- Si b divise a, alors $\text{PGCD}(a;b) = |b|$
- Soit $b \neq 0$: $\text{PGCD}(0;b) = |b|$

Démonstration

- Un entier a et sa valeur absolue $|a|$ ont les mêmes diviseurs ; donc $\text{PGCD}(a;b) = \text{PGCD}(|a|;|b|)$.
- ☐ Le plus grand diviseur d'un entier positif b est lui-même ; et le plus grand diviseur d'un entier négatif b est $-b$.
  On déduit de ceci que le plus grand diviseur d'un entier b quelconque est $|b|$.
  ☐ Si b divise a, alors bien évidemment $|b|$ divise également a.
  $|b|$ étant le plus grand diviseur de b, tout diviseur commun à a et b est inférieur à $|b|$; en particulier $\text{PGCD}(a;b) \leqslant |b|$.
  ☐ Par définition, $|b|$ étant un diviseur commun de a et b, $\text{PGCD}(a;b) \geqslant |b|$.
  ☐ Les deux points ci-dessus justifient que $\text{PGCD}(a;b) = |b|$.
- Pour justifier cette propriété, on applique le point précédent avec $a = 0$, car tout entier b non nul divise 0...

En guise d'explications

D'après le premier point de cette propriété, déterminer le PGCD de deux entiers relatifs revient à déterminer le PGCD de deux entiers naturels. Pour la suite, on considèrera que les entiers a et b dont on cherchera le PGCD sont positifs, et on ne s'intéressera qu'à leurs diviseurs positifs.

Propriété 2

Soient a et b deux entiers, et r le reste dans la division euclidienne de a par b.
Alors $D_{\mathbb{N}}(a,b) = D_{\mathbb{N}}(b,r)$

Démonstration

On note q le quotient dans la division euclidienne de a par b.

- Soit d un diviseur commun à a et b.
  On a : $a = bq + r$, d'où $r = a - bq$.
  Comme d divise a et b, d divise $a - bq$, c'est-à-dire : d divise r.

  d est donc un diviseur commun à b et r : $d \in D_{\mathbb{N}}(b,r)$.
  Autrement dit : tout élément de $D_{\mathbb{N}}(a,b)$ appartient à $D_{\mathbb{N}}(b,r)$.

- Soit d un diviseur commun à b et r.
  On a : $a = bq + r$.
  Comme d divise b et r, d divise $bq + r$, c'est-à-dire : d divise a.

  d est donc un diviseur commun à a et b : $d \in D_{\mathbb{N}}(a,b)$.
  Autrement dit : tout élément de $D_{\mathbb{N}}(b,r)$ appartient à $D_{\mathbb{N}}(a,b)$.

- Les deux points ci-dessus justifient que $D_{\mathbb{N}}(a,b) = D_{\mathbb{N}}(b,r)$.

2. Algorithme d'Euclide

Théorème 1

Soient a et b deux entiers naturels non nuls tels que b ne divise pas a. $\text{PGCD}(a;b)$ est **le dernier reste non nul** (ici noté r_n) obtenu par les divisions euclidiennes successives décrites ci-après :

Dividende	Diviseur	Reste	Division euclidienne	Encadrement du reste
a	b	r_0	$a = bq_0 + r_0$	$0 < r_0 < b$
b	r_0	r_1	$b = r_0q_1 + r_1$	$0 \leq r_1 < r_0$
r_0	r_1	r_2	$r_0 = r_1q_2 + r_2$	$0 \leq r_2 < r_1$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
r_{n-2}	r_{n-1}	r_n	$r_{n-2} = r_{n-1}q_n + r_n$	$0 \leq r_n < r_{n-1}$
r_{n-1}	r_n	0	$r_{n-1} = r_nq_{n+1} + 0$	0

$D_{\mathbb{N}}(a,b) = D_{\mathbb{N}}(b,r_0) = D_{\mathbb{N}}(r_0,r_1) = \dots\dots = D_{\mathbb{N}}(r_{n-2},r_{n-1}) = D_{\mathbb{N}}(r_{n-1},r_n) = D_{\mathbb{N}}(r_n) = D_{\mathbb{N}}(\text{PGCD}(a;b))$.

En guise d'explications ▶ sur l'algorithme d'Euclide :

- Avec la succession de divisions euclidiennes décrites ci-dessus, on a une suite de restes strictement décroissante.
  On est donc certain d'aboutir, au bout d'un certain nombre d'étapes (inférieur au premier reste r_0), à un reste égal à 0.
- La propriété précédente justifie que :

$$D_{\mathbb{N}}(a,b) = D_{\mathbb{N}}(b,r_0) = D_{\mathbb{N}}(r_0,r_1) = \dots\dots = D_{\mathbb{N}}(r_{n-2},r_{n-1}) = D_{\mathbb{N}}(r_{n-1},r_n)\,.$$

  Or r_n est un diviseur de r_{n-1} (car le reste suivant vaut 0) : donc $D_{\mathbb{N}}(r_{n-1},r_n) = D_{\mathbb{N}}(r_n)$.

  Ainsi : $D_{\mathbb{N}}(a,b) = D_{\mathbb{N}}(r_n)\,.$
- Or le plus grand élément de $D_{\mathbb{N}}(r_n)$ est r_n lui-même ;

  r_n est donc le PGCD de a et b.

Recherche

Exercice 4 : En utilisant l'algorithme d'Euclide, calculer PGCD$(1958;4539)$.

En guise d'explications

L'algorithme d'Euclide permet d'établir que les diviseurs communs à a et b sont les diviseurs de leur PGCD , car on a justifié que $D_{\mathbb{N}}(a,b) = D_{\mathbb{N}}(r_n)$.
On a ainsi la propriété suivante, qui est équivalente à la définition du PGCD :

Propriété 3

a et b sont deux entiers. Si on note $d = \text{PGCD}(a;b)$, tous les diviseurs communs à a et b divisent d.

Algorithme et Python 1

Voici l'algorithme d'Euclide en Python.
Quelle est la variable dont on renvoie la valeur en sortie ?

Codage en Python

```
1 def PGCD(a,b) :
2     while a%b>0 :
3         r=a%b
4         a,b=b,r
5     return ...
```

Algorithme disponible sur Jupyter

3. Nombres premiers entre eux

Définition 2

On dit que a et b sont **premiers entre eux** si, et seulement si, $\text{PGCD}(a;b) = 1$.

Recherche

Exercice 5 : Démontrer que 153 et 104 sont premiers entre eux.

En guise d'explications

Il ne faut pas confondre les nombres premiers et les nombres premiers entre eux. 153 et 104 ne sont pas premiers, mais ils sont premiers entre eux. Mais deux nombres premiers distincts sont premiers entre eux car les diviseurs positifs d'un nombre premier sont 1 et lui-même.

Théorème 2 ▶ Théorème de Bézout

Deux entiers a et b sont premiers entre eux, **si et seulement si,** il existe un couple $(u;v)$ d'entiers relatifs tels que

$$au + bv = 1.$$

Démonstration

- **Montrons d'abord que s'il existe deux entiers u et v tels que $au+bv = 1$, alors a et b sont premiers entre eux :**

  Soit d un diviseur positif commun de a et b ; ainsi il existe deux entiers a' et b' tels que $a = da'$ et $b = db'$.

  En remplaçant a et b dans l'égalité $au + bv = 1$, on obtient $da'u + db'v = 1$, d'où $d(a'u + b'v) = 1$: d est un diviseur de 1, donc est égal à 1.

  Le plus grand diviseur commun de a et b est donc 1.

- **Montrons maintenant que si a et b sont premiers entre eux, alors il existe deux entiers u et v tels que $au + bv = 1$:**

  Notons E l'ensemble $\{au + bv\,;\, u \in \mathbb{Z},\, v \in \mathbb{Z}\}$, et d le plus petit élément de E strictement positif.

  Comme $d \in E$, il existe deux entiers u_0 et v_0 tels que $d = au_0 + bv_0$.

  ☐ Effectuons la division euclidienne de a par d : $a = dq + r$, avec $0 \leqslant r < d$.

  Ainsi $r = a - dq$, puis $r = a - (au_0 + bv_0)q$ (en remplaçant d par $au_0 + bv_0$).

Puis $r = a - au_0q - bv_0q = a(1 - u_0q) + b(-v_0q)$: r est un élément de E, positif, et inférieur strictement à d, qui est le plus petit élément de E strictement positif :

r est nécessairement égal à 0.

Ceci prouve que d divise a.

☐ On montre exactement de la même façon que d divise b.

☐ Or a et b sont premiers entre eux : donc $d = 1$.

$1 \in E$, donc il existe deux entiers u et v tels que $au + bv = 1$.

Recherche

Exercice 6 : Montrer que $\forall n \in \mathbb{N}$, $2n + 1$ et $3n + 2$ sont premiers entre eux.

A titre d'exemple

Montrer que 59 et 27 sont premiers entre eux, puis déterminer deux entiers x et y tels que $59x + 27y = 1$.

On applique l'algorithme d'Euclide :

$$59 = 27 \times 2 + 5$$
$$27 = 5 \times 5 + 2$$
$$5 = 2 \times 2 + \textcircled{1}$$
$$2 = 1 \times 2 + 0$$

59 et 27 sont bien premiers entre eux.

La méthode indiquée ci-dessous est à retenir.
Le théorème de Bézout nous permet d'affirmer qu'il existe deux entiers x et y tels que $59x + 27y = 1$; mais il ne nous indique pas comment obtenir ces entiers x et y.
La méthode proposée ici est « la remontée de l'algorithme d'Euclide » : elle consiste à partir de la dernière division euclidienne, puis de remplacer les restes successivement obtenus.

Algorithme d'Euclide	Remontée de l'algorithme
$59 = 27 \times 2 + 5$	$1 = 5 - 2 \times 2$
$27 = 5 \times 5 + 2$	$1 = 5 - 2 \times 2$
$5 = 2 \times 2 + 1$	$1 = 5 - 2 \times (27 - 5 \times 5)$
	$1 = 5 - 2 \times 27 + (-2) \times (-5) \times 5$
	$1 = 5 - 2 \times 27 + 10 \times 5$
	$1 = 11 \times 5 - 2 \times 27$
	$1 = 11 \times 5 - 2 \times 27$
	$1 = 11 \times (59 - 27 \times 2) - 2 \times 27$
	$1 = 11 \times 59 + 11 \times (-2) \times 27 - 2 \times 27$
	$1 = 11 \times 59 - 22 \times 27 - 2 \times 27$
	$1 = 11 \times 59 - 24 \times 27$

Les valeurs $x = 11$ et $y = -24$ conviennent. *On verra plus tard qu'il y en a une infinité d'autres ...*

4. Autres propriétés du PGCD

Corollaire 1 ▶ du Théorème de Bézout

Soit $n \geqslant 2$ un entier naturel ; on rappelle que deux entiers a et b sont inverses modulo n si et seulement si $ab \equiv 1\,[n]$; un entier a est inversible modulo n s'il possède un inverse modulo n.

Soit $n \geqslant 2$ un entier naturel.
Un entier a est inversible modulo n si et seulement si a et n sont premiers entre eux.

Recherche

Exercice 7 : Déterminer tous les entiers inversibles modulo n, et préciser leur inverse, pour :

1. $n = 8$;
2. $n = 11$;
3. $n = 24$.

Corollaire 2 ▶ du Théorème de Bézout

Soient a et b deux entiers, et $d = \text{PGCD}(a; b)$.

- Il existe un couple $(u; v)$ d'entiers relatifs tels que $au + bv = d$ (Egalité de Bézout) .
- Les nombres $\dfrac{a}{d}$ et $\dfrac{b}{d}$ sont des entiers premiers entre eux.
- Soit k un entier naturel non nul : $\text{PGCD}(ka; kb) = kd$.

Démonstration

La démonstration du premier point est similaire à celle du théorème de Bézout.

- Notons E l'ensemble $\{au + bv\,;\, u \in \mathbb{Z},\, v \in \mathbb{Z}\}$, et n le plus petit élément de E strictement positif.
  Comme $n \in E$, il existe deux entiers u_0 et v_0 tels que $n = au_0 + bv_0$.
  - ☐ Effectuons la division euclidienne de a par n : $a = nq + r$, avec $0 \leqslant r < n$.
    Ainsi $r = a - nq$, puis $r = a - (au_0 + bv_0)q$ (en remplaçant n par $au_0 + bv_0$).
    Puis $r = a - au_0q - bv_0q = a(1 - u_0q) + b(-v_0q)$: r est un élément de E, positif, et inférieur strictement à n, qui est le plus petit élément de E strictement positif :
    $$r \text{ est nécessairement égal à } 0.$$
    Ceci prouve que n divise a.
  - ☐ On montre exactement de la même façon que n divise b.
  - ☐ n étant un diviseur commun à a et b, n divise leur PGCD d.
  - ☐ On rappelle qu'il existe deux entiers u_0 et v_0 tels que $n = au_0 + bv_0$; d divisant a et b, d divise n.
  - ☐ Les deux points précédents prouvent que $d = n$: donc $d = au_0 + bv_0$.
- Tout d'abord, d divisant a et b, les nombres $\dfrac{a}{d}$ et $\dfrac{b}{d}$ sont bien des entiers.
  D'après le premier point, il existe deux entiers u et v tels que $d = au + bv$; en divisant cette égalité par d, on obtient :
  $$1 = u\frac{a}{d} + v\frac{b}{d}\,.$$
  D'après le théorème de Bézout, les entiers $\dfrac{a}{d}$ et $\dfrac{b}{d}$ sont premiers entre eux.
- Soit k un entier non nul ; notons $D = \text{PGCD}(ka; kb)$.

☐ $d = \text{PGCD}(a;b)$, donc d'après le premier point il existe deux entiers u et v tels que $au + bv = d$.
En multipliant cette égalité par k, on obtient : $kau + kbv = kd$.
D étant un diviseur de ka et kb,

D est aussi un diviseur de kd.

☐ d divise a et b, donc kd divise ka et kb.
kd est donc un diviseur du PGCD de ka et kb.

kd est un diviseur de D.

☐ On conclut des deux points précédents que $D = kd$.

Recherche

Exercice 8 : Soient a et b deux entiers naturels.
Leur PGCD vaut 26 et $a \times b = 6\,084$.
Déterminer les valeurs possibles de a et b.

Recherche

Exercice 9 :
On cherche à déterminer les inverses de 7 modulo 26, c'est-à-dire l'ensemble des nombres entiers tels que

$$7x \equiv 1 \qquad [26]$$

1. Démontrer que les nombres 26 et 7 sont premiers entre eux.
2. Expliquez pourquoi il existe au moins un couple d'entiers $(u; v)$ tel que $7u + 26v = 1$. En déterminer un.
3. En déduire un inverse de 7 modulo 26.
4. En déduire la solution entière p contenue dans l'intervalle $[0; 26]$ de l'équation $9p - 8 \equiv 2p + 21 \qquad [26]$

Algorithme et Python 2

Pour deux entiers a et b, il existe deux entiers u et v tels que $au + bv = \text{PGCD}(a, b)$.
Ces entiers u et v sont appelés **coefficients de Bézout**.

L'algorithme ci-contre détermine s'il existe une valeur de u comprise entre les entiers m et n ; si c'est le cas, il renvoie le couple (u, v) tel que $au + bv = \text{PGCD}(a, b)$.

Cette fonction « coeff_bezout » appelle la fonction « PGCD » vue précédemment.

Codage en Python

```
1 def coeff_bezout(a,b,m,n) :
2     r=PGCD(a,b)−m∗a
3     while ..... and m<=n :
4         m+=1
5         r=PGCD(a,b)−m∗a
6     if r%b==0 :
7         return ..... , .....
```

```
>>> PGCD(2045,328)
1
>>> coeff_bezout(2045,328,0,100)
>>> coeff_bezout(2045,328,−2000,100)
(−1755, 10942)
```

- 2 045 et 328 sont premiers entre eux.
- Il n'existe pas d'égalité de Bézout $2\,045u + 328v = 1$ avec $0 \leqslant u \leqslant 100$.
- $-1\,755$ est bien compris entre $-2\,000$ et 100, et on a bien $2\,045 \times -1\,755 + 328 \times 100 = 1$.

Algorithme disponible sur Jupyter

5. Théorèmes de Gauss

Théorème 3 ▶ le premier

Soient a, b et c trois entiers relatifs non nuls.

Si a divise le produit bc et si a et b sont premiers entre eux, alors a divise c.

Démonstration

a et b étant premiers entre eux, il existe d'après le théorème de Bézout deux entiers u et v tels que $au + bv = 1$.
En multipliant cette égalité par c, on obtient $cau + cbv = c$.
Or a divise bc : il existe un entier d tel que $ad = bc$.
En remplaçant cb par ad dans l'égalité de Bézout, on obtient :

$$cau + adv = c\,,$$

puis en factorisant par a,

$$a(cu + dv) = c \text{ avec } cu + dv \text{ entier ; donc } a \text{ divise } c\,.$$

Propriété 4

Un quotient d'entiers naturels ne peut s'écrire sous forme irréductible que d'une seule façon

Démonstration

On considère deux fractions irréductibles égales d'entiers naturels : $\dfrac{a}{b} = \dfrac{c}{d}$; on suppose donc que a et b sont premiers entre eux, et que c et d sont premiers entre eux
Montrons alors que $a = c$ et $b = d$.

On déduit de $\dfrac{a}{b} = \dfrac{c}{d}$ l'égalité suivante : $ad = bc$.

Ainsi a divise bc.
Or a est premier avec b ; d'après le premier théorème de Gauss, a divise c : il existe un entier naturel k tel que $c = ka$.

En remplaçant c par ka dans l'égalité $ad = bc$, on obtient $ad = bka$, puis, en simplifiant par a (qui n'est pas nul), on a : $d = kb$.

On a montré qu'il existe un entier naturel k tel que $c = ka$ et $d = kb$: k est donc un diviseur commun de c et d.
c et d étant deux entiers naturels premiers entre eux, nous en déduisons que $k = 1$.

Donc $d = b$ et $c = a$.

Théorème 4 ▶ le deuxième

Soient a, b et c trois entiers relatifs non nuls.

Si b et c divisent a et si b et c sont premiers entre eux, alors bc divise a.

Démonstration

c et b étant premiers entre eux, il existe d'après le théorème de Bézout deux entiers u et v tels que $cu + bv = 1$.
En multipliant cette égalité par a, on obtient $acu + abv = a$.
Or b divise a : il existe un entier d tel que $bd = a$;
et c divise a : il existe un entier d' tel que $cd' = a$.
En remplaçant a judicieusement dans l'égalité $acu + abv = a$, on obtient :

$$bdcu + cd'bv = a\,,$$

puis en factorisant par bc,

$$bc(du + d'v) = a \text{ avec } du + d'v \text{ entier ; donc } bc \text{ divise } a\,.$$

6. Résolution des équations diophantiennes $ax + by = c$

En guise d'explications

Il s'agit de résoudre l'équation $ax + by = c$, d'inconnues entières x et y.

Propriété 5

- Si PGCD$(a;b)$ ne divise pas c, alors l'équation n'a aucune solution.
- Si PGCD$(a;b)$ divise c, alors l'équation a une infinité de solution.

Démonstration

Notons d le PGCD de a et b.

- Si PGCD$(a;b)$ ne divise pas c :

  S'il existait un couple d'entiers $(x;y)$ vérifiant $ax+by=c$, alors, comme d divise $ax+by$ (car d divise a et b), d diviserait c : or ce n'est pas le cas.

  Ceci prouve par l'absurde que l'équation $ax+by=c$ n'admet aucune solution.

- Si PGCD$(a;b)$ divise c :

  Il existe un entier q tel que $c=dq$.

  Il existe également un couple d'entiers u et v tels que $au+bv=d$, car d est le PGCD de a et b.

  En multipliant cette égalité de Bézout par q, on obtient :

  $$a(qu)+b(qv)=qd=c\,;\ \text{le couple } (qu,qv) \text{ est solution .}$$

  On a déjà une solution.

  On peut montrer que pour tout entier k, les couples $(qu+kb;qv-ka)$ sont également solutions, car :

  $$a(qu+kb)+b(qv-ka)=aqu+kab+bqv-kab=aqu+bqv=c\,.$$

  Remarque : Tous les couples proposés ci-dessus sont solutions ; cela ne signifie pas que tous les couples solutions s'écrivent de cette forme...

A titre d'exemple

PGCD$(21;15)=3$; ainsi l'équation diophantienne $21x+15y=4$ n'a aucune solution.

Méthode ▶ Résolution des équations diophantiennes :

$$11x-4y=1 \qquad 7x-5y=9 \qquad 15x+6y=18$$

Résolution de $11x-4y=1$ *:*

1ère étape : Déterminons le PGCD de 11 et -4, qui est celui de 11 et 4 (par l'algorithme d'Euclide ou une autre méthode).

$$\begin{aligned}11&=4\times2+3\\4&=3\times1+\textcircled{1}\\3&=1\times3+0\end{aligned}$$

Ce PGCD vaut 1 ; cette équation admet une infinité de solutions.

2ème étape : Déterminer une égalité de Bézout (par la remontée de l'algorithme d'Euclide ou une autre méthode).

$$\begin{aligned}1&=4-3\\1&=4-(11-4\times2)\\1&=4-11+4\times2\\1&=4\times3+11\times(-1)\end{aligned}$$

3ème étape : Déduire de l'égalité de Bézout une solution de l'équation.

$$11 \times (-1) - 4 \times (-3) = 1 \text{ : le couple } (-1;-3) \text{ est solution.}$$

4ème étape : A l'aide de la solution particulière et du premier lemme de Gauss, déterminer la forme d'une des deux inconnues.

Soit $(x;y)$ un couple solution de l'équation $11x - 4y = 1$; le couple $(-1;-3)$ étant également solution, car $11 \times (-1) - 4 \times (-3) = 1$, on a :

$$11x - 4y = 11 \times (-1) - 4 \times (-3)\,.$$

En faisant passer certains termes de l'autre côté, on obtient :

$$11x - 11 \times (-1) = -4 \times (-3) + 4y$$

puis, en factorisant,

$$11(x+1) = 4(y+3) \ (*).$$

- 11 divise $4(y+3)$;
- 11 est premier avec 4.

D'après le lemme de Gauss, 11 divise $y+3$: il existe un entier k tel que $y+3 = 11k$, c'est-à-dire : $y = 11k - 3$.

5ème étape : Déterminer la forme de la deuxième inconnue.

En remplaçant $y+3$ par $11k$ dans l'équation $(*)$, on obtient :

$$11(x+1) = 4 \times 11k$$

puis, en simplifiant par 11 :

$$x + 1 = 4k \text{ c'est-à-dire } x = 4k - 1\,.$$

6ème étape : Vérifier que les couples de cette forme sont tous solutions.

Soit k un entier :
$11(4k-1) - 4(11k-3) = 11 \times 4k - 11 - 4 \times 11k - 4 \times (-3) = 44k - 11 - 44k + 12 = 1.$
Les couples $(4k-1;11k-3)$ (où $k \in \mathbb{Z}$) sont bien solutions de l'équation $11x - 4y = 1$.

Conclusion : Les solutions de l'équation $11x - 4y = 1$ sont les couples $(4k-1;11k-3)$, où $k \in \mathbb{Z}$.

Résolution de $7x - 5y = 9$:

1ère étape : Déterminons le PGCD de 7 et -5, qui est celui de 7 et 5 (par l'algorithme d'Euclide ou une autre méthode).

$$7 = 5 \times 1 + 2$$
$$5 = 2 \times 2 + (1)$$
$$2 = 1 \times 2 + 0$$

Ce PGCD vaut 1 ; cette équation admet une infinité de solutions.

2ème étape : Déterminer une égalité de Bézout (par la remontée de l'algorithme d'Euclide ou une autre méthode).

$$1 = 5 - 2 \times 2$$
$$1 = 5 - (7 - 5 \times 1)2$$
$$1 = 5 - 7 \times 2 + 5 \times 2$$
$$1 = 5 \times 3 + 7 \times (-2)$$

3ème étape : Déduire de l'égalité de Bézout une solution de l'équation.

$$7 \times (-2) - 5 \times (-3) = 1$$

En multipliant par 9, on obtient :

$$7 \times (-18) - 5 \times (-27) = 9 \text{ : le couple } (-18; -27) \text{ est solution.}$$

4ème étape : A l'aide de la solution particulière et du premier lemme de Gauss, déterminer la forme d'une des deux inconnues.

Soit $(x; y)$ un couple solution de l'équation $7x - 5y = 9$; le couple $(-18; -27)$ étant également solution, car $7 \times (-18) - 5 \times (-27) = 9$, on a :

$$7x - 5y = 7 \times (-18) - 5 \times (-27)\,.$$

En faisant passer certains termes de l'autre côté, on obtient :

$$7x - 7 \times (-18) = -5 \times (-27) + 5y$$

puis, en factorisant,

$$7(x + 18) = 5(y + 27) \ (*).$$

- 7 divise $5(y + 27)$;
- 7 est premier avec 5.

D'après le lemme de Gauss, 7 divise $y + 27$: il existe un entier k tel que $y + 27 = 7k$, c'est-à-dire : $y = 7k - 27$.

5ème étape : Déterminer la forme de la deuxième inconnue.

En remplaçant $y + 27$ par $7k$ dans l'équation $(*)$, on obtient :

$$7(x + 18) = 5 \times 7k$$

puis, en simplifiant par 7 :

$$x + 18 = 5k \text{ c'est-à-dire } x = 5k - 18\,.$$

6ème étape : Vérifier que les couples de cette forme sont tous solutions.

Soit k un entier :
$7(5k - 18) - 5(7k - 27) = 7 \times 5k - 126 - 5 \times 7k + 135 = 35k - 126 - 35k + 135 = 9.$
Les couples $(5k - 18; 7k - 27)$ (où $k \in \mathbb{Z}$) sont bien solutions de l'équation $7x - 5y = 9$.

Conclusion : Les solutions de l'équation $7x - 5y = 9$ sont les couples $(5k - 18; 7k - 27)$, où $k \in \mathbb{Z}$.

Résolution de $15x + 6y = 18$ *:*

1ère étape : Déterminons le PGCD de 15 et 6 (par l'algorithme d'Euclide ou une autre méthode).

$$15 = 6 \times 2 + 3$$
$$6 = 3 \times 2 + 0$$

Ce PGCD vaut 3 ; comme 3 divise 18, cette équation admet une infinité de solutions.

2ème étape : Déterminer une égalité de Bézout (par la remontée de l'algorithme d'Euclide ou une autre méthode).

$$3 = 15 - 6 \times 2$$

3ème étape : Déduire de l'égalité de Bézout une solution de l'équation.

$$15 \times 1 + 6 \times (-2) = 3$$

En multipliant par 6, on obtient :

$$15 \times 6 + 6 \times (-12) = 18 \text{ : le couple } (6; -12) \text{ est solution.}$$

4ème étape : A l'aide de la solution particulière et du premier lemme de Gauss, déterminer la forme d'une des deux inconnues.

Soit $(x; y)$ un couple solution de l'équation $15x + 6y = 18$; le couple $(6; -12)$ étant également solution, car $15 \times 6 + 6 \times (-12) = 18$, on a :

$$15x + 6y = 15 \times 6 + 6 \times (-12)\,.$$

En faisant passer certains termes de l'autre côté, on obtient :

$$15x - 15 \times 6 = 6 \times (-12) - 6y$$

puis, en factorisant,

$$15(x - 6) = 6(-y - 12)$$

et enfin en simplifiant par 3,

$$5(x - 6) = 2(-y - 12) \quad (*).$$

- 5 divise $2(-y - 12)$;
- 5 est premier avec 2.

D'après le lemme de Gauss, 5 divise $-y-12$: il existe un entier k tel que $-y-12 = 5k$, c'est-à-dire : $y = -5k-12$.

5ème étape : Déterminer la forme de la deuxième inconnue.

En remplaçant $-y - 12$ par $5k$ dans l'équation $(*)$, on obtient :

$$5(x - 6) = 2 \times 5k$$

puis, en simplifiant par 5 :

$$x - 6 = 2k \text{ c'est-à-dire } x = 2k + 6\,.$$

6ème étape : Vérifier que les couples de cette forme sont tous solutions.

Soit k un entier :
$15(2k + 6) + 6(-5k - 12) = 15 \times 2k + 90 + 6 \times (-5k) - 72 = 30k + 90 - 30k - 72 = 18.$
Les couples $(2k + 6; -5k - 12)$ (où $k \in \mathbb{Z}$) sont bien solutions de l'équation $15x + 6y = 18$.

Conclusion : Les solutions de l'équation $15x + 6y = 18$ sont les couples $(2k + 6; -5k - 12)$, où $k \in \mathbb{Z}$.

Recherche

Problème

Lors d'un trek, un marcheur a effectué des réservations dans deux types de gîtes : le gîte A et le gîte B.
Une nuit dans le gîte A coûte 24 € et une nuit dans le gîte B coûte 45 €.
Il se rappelle que le coût total de sa réservation est de 885€.
On souhaite retrouver les nombres x et y de nuitées passées respectivement dans le gîte A et dans le gîte B

1. Montrer que les nombres x et y sont respectivement inférieurs ou égaux à 36 et 19.

2. Justifier que le coût total de la réservation est un multiple de 3.

3. a) Justifier que l'équation $8x + 15y = 1$ admet pour solution au moins un couple d'entiers relatifs.
   En déterminer un.

b) En déduire une solution $(x_0; y_0)$ de l'équation $8x + 15y = 295$.

c) Démontrer que (x, y) est solution de $8x + 15y = 295$ si et seulement si $8(x - x_0) = -15(y - y_0)$.

d) En déduire l'ensemble des solutions de $8x + 15y = 295$.

e) Expliquez pourquoi résoudre le problème revient à résoudre l'équation (E) : $8x + 15y = 295$ où x et y sont des nombres entiers relatifs vérifiant $0 \leqslant x \leqslant 36$ et $0 \leqslant y \leqslant 19$.

f) Compléter les pointillés afin que le programme Python retourne une solution du problème.

Codage en Python

```
def bezout() :
    for x in range(.....) :
        for y in range(.....) :
            if ..... :
                return(x,y)
```

g) Programmer la fonction Bezout puis déterminer une solution possible du problème.

.....
.....
.....
.....
.....
.....

4. Le randonneur se souvient avoir passé entre 10 et 20 nuits dans le gîte A. Déterminer le nombre exact de nuits passées dans le gîte A et celui des nuits passées dans le gîte B.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

7. Plus Petit Multiple Commun

Définition 3

Soient a et b deux entiers relatifs non nuls.
L'ensemble des multiples strictement positifs communs à a et b admet un plus petit élément appelé le **plus petit multiple commun**. On le note : PPCM$(a;b)$.

Recherche

Exercice 10 : Déterminer PPCM(60 ;84),en dressant la liste des premiers multiples positifs de ces entiers.

Propriété 6

Soient a et b deux entiers naturels non nuls.

- Si b divise a, alors PPCM$(a;b) = a$.
- PPCM$(a;b) = \dfrac{ab}{\text{PGCD}(a;b)}$; en particulier, si a et b sont premiers entre eux, PPCM$(a;b) = ab$.

Démonstration

- Si b divise a, a est un multiple de b ; or $a \times 1$ est le plus petit multiple strictement positif de a ; donc le PPCM de a et b est a.
- Notons d le PGCD de a et b.

  ☐ Tout d'abord, on peut remarquer que $\frac{a}{d}$ et $\frac{b}{d}$ sont entiers, donc $b \times \frac{a}{d}$ est un multiple de b, et $a \times \frac{b}{d}$ un multiple de a.

  Bien sûr, $b \times \frac{a}{d} = a \times \frac{b}{d} = \frac{ab}{d}$: ce nombre est donc un multiple commun de a et b.

  ☐ Nous allons maintenant montrer que tout multiple commun de a et b est un multiple de $\frac{ab}{d}$:

  Soit m un multiple commun de a et b, on peut écrire que $m = ka = qb$ avec k et q entiers naturels.
  Comme d est le PGCD de a et b, on peut aussi écrire que $a = da'$ et $b = db'$, avec a' et b' premiers entre eux.
  D'où $kda' = qdb'$, ce qui équivaut à $ka' = qb'$.
  Comme a' et b' sont premiers entre eux, d'après le théorème de Gauss, a' divise q : donc il existe un entier naturel n tel que $q = na'$.
  Or $m = qb$: donc $m = na'b = n\frac{a}{d}b$: m est un multiple de $\frac{ab}{d}$, donc $m \geqslant \frac{ab}{d}$.

En guise d'explications

- Dans le démonstration du second point, on a montré que les multiples communs à a et b sont les multiples communs de leur PPCM.
- Quand on réduit deux fractions au même dénominateur, la plus petite valeur possible de ce dénominateur commun est le PPCM des deux dénominateurs.