Math93.com

Arithmétique Partie 2

Tle Maths Experte

I. PGCD de deux nombres entiers (*gcd in english*)

Définition 1

Soient a et b deux entiers relatifs non simultanément nuls. L'ensemble des diviseurs communs à a et b est une partie non vide de $\mathbb{Z}$ (elle contient 1) et majorée (par le maximum entre $|a|$ et $|a|$).
Cet ensemble admet un plus grand élément appelé Plus Grand Diviseur Commun de a et b.
On le note $PGCD(a,b)$ ou parfois $a \wedge b$.

Remarque

- on a : $PGCD(a,b) = PGCD(b,a)$.
- On utilise le lemme suivant : « Toute partie non vide et majorée de $\mathbb{Z}$ admet un unique plus grand élément. »

Exemple

Déterminer le $PGCD$ de 30 et de -12. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

Propriété 1

Soient a et b deux entiers relatifs non simultanément nuls.
On a PGCD $(a\,;b)$ = PGCD $(|a|\,;|b|)$ et pour tout couple $(a\,;b) \in \mathbb{N}^2$ avec $a \neq 0$:

1. $\boxed{\text{PGCD}(a\,;b) \geqslant 1}$, $\boxed{\text{PGCD}(a\,;0) = a}$ et $\boxed{\text{PGCD}(a\,;1) = 1}$.
2. a divise b si et seulement si PGCD $(a\,;b) = a$.

$$\boxed{\text{PGCD}(a\,;b) = a \iff a|b}$$

3. Méthode de soustraction (avec $a \geqslant b$) :

$$\boxed{\text{PGCD}\,(a\,;b) = \text{PGCD}\,(a-b\,;b)}$$

Preuve

On note P le PGCD de a et b.

1. $\text{PGCD}(a\,;b) \geqslant 1$, $\text{PGCD}(a\,;0) = a$ et $\text{PGCD}(a\,;1) = 1$.
   - 1 est un diviseur commun à tous les entiers, donc le plus grand commun diviseur de deux entiers est au moins égal à 1 (donc positif).
   - Si $b = 0$, alors P est un diviseur commun à a et 0. Or a est un diviseur commun à lui-même et 0. Comme a est le plus grand diviseur de a, $P = a$.
   - Si $b = 1$, alors le plus grand diviseur de b est 1. De plus 1 divise aussi a. Donc $P = 1$.

2. a divise b si et seulement si PGCD $(a\,;b) = a$.

- Si $a|b$, alors a est un diviseur commun à a et b. Et comme a est son plus grand diviseur, on a $P = a$.
- réciproquement si $P = a$, alors a est un diviseur commun à a et b. En particulier, $a|b$.
- On a donc, au final, démontré l'équivalence :

$$P = a \iff a|b$$

3. Méthode de soustraction :

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

- Supposons que $a \geqslant b$. Puisque P divise a et b, alors P divise $a-b$. Ainsi, P est un diviseur commun à $a-b$ et b, et donc $P \leqslant PGCD(a-b\,;\,b)$.
- Réciproquement, si d est un diviseur commun à $a-b$ et b, alors d divise $(a-b)+b = a$, donc d est un diviseur commun à a et b.
  En particulier, $PGCD(a-b\,;\,b)$ est un diviseur commun à a et b, donc $PGCD(a-b\,;\,b)?P$.
- On vient de montrer qu'on a à la fois $P \leqslant PGCD(a-b\,;\,b)$ et $PGCD(a-b\,;\,b) \leqslant P$ donc, en conclusion, $P = PGCD(a-b\,;\,b)$.

II. Détermination rapide du PGCD

Dans cette partie, a et b sont deux entiers naturels non nuls avec $a > b$.

II.1 Lemme d'Euclide

Propriété 2

a, b, q et r sont des entiers relatifs non nuls.
On note q et r le quotient et le reste de la division euclidienne de a par b.

$$a = bq + r \quad ; \quad 0 \leqslant r < b$$

Avec ces notations,

$$\boxed{PGCD(a\,;\,b) = PGCD(b\,;\,r)}.$$

On a aussi : l'ensemble des diviseurs de a et de b est égal à l'ensemble des diviseurs de b et de r.

Preuve

- Soit d un diviseur commun à a et b. Par définition, $a = bq + r$ donc $r = a - bq$.
  r s'écrit donc comme une combinaison linéaire de a et de b et d divise à la fois a et b.
  Donc d divise r.
  En particulier, d est un diviseur commun à b et r.
- De même, a est une combinaison linéaire de b et r, donc tout diviseur commun à b et r divise a.
- Ainsi, l'ensemble des diviseurs communs à a et b est confondu avec l'ensemble des diviseurs communs à b et r. Ils ont donc le même plus grand élément d'où

$$PGCD(a\,;\,b) = PGCD(b\,;\,r)$$

.

II.2 Algorithme d'Euclide

a et b sont deux entiers naturels non nuls avec $a > b$.

Propriété 3

a et b sont deux entiers naturels non nuls avec $a > b$.

- Si b divise a, le $PGCD$ de a et de b est égal à b.
- Si b ne divise pas a, le $PGCD$ de a et de b est le dernier reste non nul dans l'exécution de l'algorithme d'Euclide.

Exercice 1

Déterminer, avec l'algorithme d'Euclide, le $PGCD$ de 6 825 et 15 675.

Correction

Calculons par l'algorithme d'EUCLIDE le PGCD des nombres 15675 et 6825.
Cet algorithme porte le nom du mathématicien grec *Euclide de Samos* (vers 300 av. J.-C.), auteur des « *Eléments* ». Il est basé sur la propriété suivante :

Propriété 4

Pour a, b entiers tels que $a \geqslant b > 0$ et r le reste de la division euclidienne de a par b :

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

Par divisions euclidiennes successives on obtient :

$$15675 = 6825 \times 2 + 2025$$
$$6825 = 2025 \times 3 + 750$$
$$2025 = 750 \times 2 + 525$$
$$750 = 525 \times 1 + 225$$
$$525 = 225 \times 2 + 75$$
$$225 = 75 \times 3 + 0$$

Le PGCD des nombres 15675 et 6825 est le dernier reste non nul du procédé, c'est-à-dire 75.

$$\boxed{\text{PGCD}\,(15675\,;\,6825) = 75}$$

On peut vérifier que 75 divise bien 15675 et 6825 :

$$15675 \div 75 = 209 \text{ et } 6825 \div 75 = 91$$

Exercice 2

Compléter cette fonction Python qui traduit l'algorithme d'Euclide :

```
def pgcd(a,b):
        if b > a : # on échange a et b si b > a
                a,b = b,a
        while b != 0:
                reste = a%b
                a = b
                b = reste
        return a
```

III. Des propriétés utiles

Propriété 5

a, b et $\lambda a + b$ sont des entiers naturels non nuls. Alors

$$\boxed{PGCD(a,b) = PGCD(a, \lambda a + b)}$$

.

Exercice 3

n est un entier naturel non nul. Quel est le $PGCD$ de n et $n+2$?

Correction

Soit n un entier naturel non nul. Nous cherchons à déterminer le plus grand commun diviseur (PGCD) de n et $n+2$.

$$\text{PGCD}(n, n+2)$$

En utilisant une propriété des PGCD, nous savons que pour tous entiers a et b, le PGCD de a et b est le même que le PGCD de a et $b-a$, c'est-à-dire :

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

Dans notre cas, cela donne :

$$\text{PGCD}(n, n+2) = \text{PGCD}(n, (n+2)-n) = \text{PGCD}(n, 2)$$

Le PGCD de n et 2 dépend de la parité de n :

- Si n est pair, alors n est divisible par 2, donc $\text{PGCD}(n,2) = 2$.
- Si n est impair, alors n n'est pas divisible par 2, donc $\text{PGCD}(n,2) = 1$.

Ainsi, le PGCD de n et $n+2$ est :

$$\text{PGCD}(n, n+2) = \begin{cases} 1 & \text{si } n \text{ est impair,} \\ 2 & \text{si } n \text{ est pair.} \end{cases}$$

Propriété 6

a, b et k sont des entiers naturels non nuls. Alors

$$\boxed{PGCD(ka, kb) = k \times PGCD(a,b)}$$

Preuve

- Étape 1 :

  La division euclidienne de a par b s'écrit

  $$a = qb + r \quad \text{avec } 0 \leqslant r < b.$$

  En multipliant cette égalité par $k \in \mathbb{N}^*$, on obtient

  $$ka = q\,(kb) + kr.$$

  Puisque $r < b$, il suit que $kr < kb$, ce qui montre que l'égalité précédente est la division euclidienne de ka par kb.

- Étape 2 : On sait que $\text{PGCD}(a,b)$ est le dernier reste non nul dans la suite des restes obtenus par l'algorithme d'Euclide. Soit $(r_n)_{n\geqslant 0}$ la suite des restes construite par cet algorithme appliqué aux entiers a et b, et soit $m \geqslant 0$ l'entier tel que

$$r_m \neq 0 \quad \text{et} \quad r_{m+1} = 0.$$

Alors,

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

D'après ce qui précède, on a

$$\text{PGCD}(ka,kb) = \text{PGCD}(kb,kr_0) = \cdots = \text{PGCD}(kr_m,kr_{m+1}) = kr_m,$$

puisque $r_{m+1} = 0$. On en déduit que

$$\text{PGCD}(ka,kb) = k\,\text{PGCD}(a,b).$$

□

Propriété 7

Soient a et b deux entiers non simultanément nuls.
d est un diviseur commun à a et b si, et seulement si, d divise $PGCD(a;b)$.

Preuve

- Soit $d \in \mathbb{Z}$ est un diviseur commun de a et b.

Soit $(a,b) \in \mathbb{Z}^2$.

On suppose que a et b ne sont pas simultanément nuls et que $d \in \mathbb{Z}$ est un diviseur commun de a et b. On sait qu'il en existe au moins un, 1 (même si ils sont premiers entre eux).

Nous allons montrer que d divise $\text{PGCD}(a,b)$ en prouvant par récurrence que d divise tous les restes obtenus par l'algorithme d'Euclide.

  - **Initialisation.** Soient q et r_0 respectivement le quotient et le reste de la division euclidienne de a par b. On a alors
$$r_0 = a - bq.$$
Puisque r_0 est une combinaison linéaire de a et b, il en découle que d divise r_0.
  - **Hérédité.** Supposons que nous avons construit la suite des restes $r_0, r_1, \ldots, r_m$ de sorte que, pour tout $k \in \{1,\ldots,m-1\}$, le terme r_{k+1} est le reste de la division euclidienne de r_{k-1} par r_k, et que d divise à la fois r_{m-1} et r_m. D'après la division euclidienne, on a
$$r_{m-1} = q_m\, r_m + r_{m+1},$$
ce qui s'écrit
$$r_{m+1} = r_{m-1} - q_m\, r_m.$$
Comme d divise r_{m-1} et r_m, il divise aussi r_{m+1} par linéarité.
  - **Conclusion.** Par récurrence, pour tout $k \in \{1,\ldots,m\}$, le reste r_k est divisible par d. Comme $\text{PGCD}(a,b)$ est le dernier terme non nul de cette suite, il en résulte que d divise $\text{PGCD}(a,b)$.

- Réciproquement :

si d divise $\text{PGCD}(a,b)$, alors, puisque $\text{PGCD}(a,b)$ divise a et b, par transitivité d divise aussi a et b.

- En conclusion, les diviseurs de $\text{PGCD}(a,b)$ sont exactement les diviseurs communs à a et b.

Exercice 4

n est un entier naturel tel que $n \equiv 1(7)$.
Parmi les réponses suivantes, quelle est celle qui donne le $PGCD$ de $3n+4$ et $4n+3$?

1, $n-1$ ou 7 ?

Correction

Soit $n \equiv 1 \pmod 7$. On peut écrire $n = 7k+1$ pour un certain $k \in \mathbb{N}$.
Calculons :

$$3n+4 = 3(7k+1)+4 = 21k+3+4 = 21k+7 = 7(3k+1),$$

$$4n+3 = 4(7k+1)+3 = 28k+4+3 = 28k+7 = 7(4k+1).$$

On a ainsi

$$\text{PGCD}(3n+4, 4n+3) = \text{PGCD}\big(7(3k+1),\, 7(4k+1)\big) = 7\,\text{PGCD}(3k+1, 4k+1).$$

Observons que

$$(4k+1)-(3k+1) = k.$$

Donc, tout diviseur commun de $3k+1$ et $4k+1$ divise k. Mais alors, il divise aussi

$$(3k+1)-3k = 1,$$

ce qui montre que $\text{PGCD}(3k+1, 4k+1) = 1$.
Par conséquent,

$$\text{PGCD}(3n+4, 4n+3) = 7 \times 1 = 7.$$

La réponse correcte est donc 7.

IV. Nombres premiers entre eux

Définition 2

Deux entiers relatifs non nuls sont **premiers entre eux** à condition que leur $PGCD$ soit égal à 1.

Exemple

18 et 35 sont premiers entre eux car 35 est un multiple de 1 ;5 ;7 et 35 alors que 18 n'est divisible par aucun de ces nombres autres que 1. Donc le PGCD de 18 et 35 vaut 1.

Propriété 8

Soient a et b deux entiers relatifs non nuls.

- Soient $d = \text{PGCD}(a, b)$ et a', b' les entiers tels que $a = da'$ et $b = db'$.
  Alors, a' et b' sont premiers entre eux.
- Réciproquement, s'il existe $d \in \mathbb{N}$ et a', b' des entiers premiers entre eux tels que $a = da'$ et $b = db'$, alors d est le PGCD de a et b.

Preuve

- Soient $d' = \text{PGCD}(a', b')$ et k_1 et k_2 les entiers tels que $a' = d'k_1$ et $b' = d'k_2$.
  On doit montrer que $d = 1$.
  En effet, $a = dd'k_1$ et $b = dd'k_2$, donc dd' est un diviseur commun à a et b.
  Comme $d = \text{PGCD}(a, b)$, on a nécessairement $dd' \leqslant d$.
  Donc, puisque $d > 0$, on en déduit que $d' = 1$.
- Réciproquement, on a :
  $$\text{PGCD}(a, b) = \text{PGCD}(da', db') = d \cdot \text{PGCD}(a', b') = d$$
  car a' et b' sont premiers entre eux.

Exercice 5

n est un entier naturel. Montrer que $2n + 3$ et $n + 3$ sont premiers entre eux **si et seulement si** n n'est pas un multiple de 3.

Correction

Nous devons démontrer que $2n + 3$ et $n + 3$ sont premiers entre eux si et seulement si n n'est pas un multiple de 3.
Posons :
$$a = 2n + 3, \quad b = n + 3$$
Nous cherchons à déterminer dans quelles conditions $\text{PGCD}(a, b) = 1$.

- Utilisation de l'algorithme d'Euclide
  Le pgcd de a et b reste invariant par soustraction de multiples de b :
  $$\text{PGCD}(a, b) = \text{PGCD}(2n + 3, n + 3)$$
  Calculons $a - 2b$:
  $$a - 2b = (2n + 3) - 2(n + 3)$$

$$= 2n + 3 - 2n - 6$$

$$= -3$$

Ainsi :

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

- Interprétation du résultat

  PGCD$(n + 3, 3)$ dépend de la divisibilité de $n + 3$ par 3 :

  - Si $n + 3$ est un multiple de 3, alors PGCD$(n + 3, 3) = 3$, donc a et b ne sont pas premiers entre eux.
  - Si $n + 3$ n'est pas un multiple de 3, alors PGCD$(n + 3, 3) = 1$, donc a et b sont premiers entre eux.
  - Reformulation en termes de n

    $n+3$ est un multiple de 3 si et seulement si n est un multiple de 3 (car $n \equiv 0 \pmod 3 \Rightarrow n+3 \equiv 0 \pmod 3$).

    Donc :
  - Si n est un multiple de 3 , alors a et b ne sont pas premiers entre eux.
  - Si n n'est pas un multiple de 3 , alors a et b sont premiers entre eux.

- Conclusion

  Nous avons démontré que $2n + 3$ et $n + 3$ sont premiers entre eux si et seulement si n n'est pas un multiple de 3.

V. Théorèmes de Bachet-Bézout

V.1 Théorème de Bézout (Admis)

Théorème 1 (Bézout, 1730-1883 / Bachet, 1581-1638)

Deux entiers naturels a et b sont premiers entre eux, si et seulement si, il existe deux entiers u et v tels que $au + bv = 1$.

Soit :

$$\boxed{\text{PGCD}\,(a\ ;\ b) = 1 \iff \exists\,(u\ ;\ v) \in \mathbb{Z}^2\ ;\ au + bv = 1}$$

Remarque : C'est le groupe Bourbaki qui attribue, vers 1948, le nom de Bézout à ce théorème, bien que celui-ci ait été énoncé et démontré par le mathématicien français Claude-Gaspard Bachet de Méziriac (1581-1638) dans son ouvrage *Problèmes plaisants et délectables*, publié en 1624. Bézout, quant à lui, établit en 1764 une généralisation de ce théorème aux polynômes dans un mémoire présenté à l'Académie des sciences.

Remarque

Il n'y a pas unicité des entiers u et v tels que $au + bv = 1$.

Méthode

Comment déterminer **un** couple $(u\ ;\ v)$ dont l'existence est assurée par l'identité de Bézout ?
Il suffit de "remonter" l'algorithme d'Euclide.

Exercice 6

Soit $a = 197$ et $b = 56$. Déterminer en appliquant l'algorithme d'Euclide un couple $(u\ ;\ v)$ tel que $au + bv = 1$.

Correction

Par divisions euclidiennes successives on obtient avec $a = 197$ et $b = 56$:

Division euclidienne	**Reste**	**Egalité avec a et b**
$197 = 56 \times 3 + 29$	$29 = 197 - 3 \times 56$	$29 = a - 3\,b$
$56 = 29 \times 1 + 27$	$27 = 56 - 1 \times 29$	$27 = b - 1 \times (a - 3\,b)$ $27 = -1\,a + 4\,b$
$29 = 27 \times 1 + 2$	$2 = 29 - 1 \times 27$	$2 = (1\,a - 3\,b) - 1 \times (-1\,a + 4\,b)$ $2 = 2\,a + (-7)\ b$
$27 = 2 \times 13 + 1$	$1 = 27 - 13 \times 2$	$1 = (-1\,a + 4\,b) - 13 \times (2\,a - 7\,b)$ $1 = -27\,a + 95\,b$

Le PGCD des nombres 197 et 56 est le dernier reste non nul du procédé, c'est-à-dire 1.
Les nombres 197 et 56 sont donc premiers entre eux et le théorème 1 dit de Bézout-Bachet assure donc l'existence de couples $(u\ ;\ v)$ d'entiers relatifs solutions de l'équation :

$$197\,u + 56\,v = 1$$

Pour trouver une solution, il suffisait d'exprimer le reste de la division euclidienne en fonction de a et b pour chaque ligne du procédé. Un couple solution de l'équation $197\,u + 56\,v = 1$ est donc :

$$\boxed{(u = -27\ ;\ v = 95)}$$

Exercice 7

n est un entier naturel. On pose : $a = 3n + 4$ et $b = 2n + 3$.
Montrer que a et b sont premiers entre eux.

Correction

Cherchons une combinaison linéaire qui élimine n.
Nous avons :

$$a = 3n + 4, \quad b = 2n + 3$$

- Construction de la combinaison $2a - 3b$

  Multipliant a par 2 et b par 3 :

$$2a = 2(3n + 4) = 6n + 8$$

$$3b = 3(2n + 3) = 6n + 9$$

  Faisons la soustraction :

$$2a - 3b = (6n + 8) - (6n + 9)$$

$$= 6n + 8 - 6n - 9$$

$$= -1$$

- Nous avons trouvé que :

$$2a - 3b = -1 \iff (-2)a + 3b = 1$$

  Donc une combinaison linéaire de a et b donne ± 1. Par le théorème de Bézout , cela prouve que a et b sont premiers entre eux.

V.2 Identité de Bézout et applications

Propriété 9

a et b sont deux entiers relatifs non nuls.
Si d est le PGCD de a et de b, **alors** il existe deux entiers relatifs u et v tels que $au + bv = d$.

Ce que l'on peut écrire :

$$\boxed{a \wedge b = d \Longrightarrow \exists (u\ ;\ v) \in \mathbb{Z}^2\ \ ,\ \ au + bv = d}$$

Preuve

Soient a et b deux entiers relatifs non nuls et posons $d = \text{PGCD}(a, b)$.
Il existe deux entiers a' et b' tels que $a = a'd$ et $b = b'd$, avec $\text{PGCD}(a', b') = 1$.
D'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tels que :

$$a'u + b'v = 1.$$

On a alors :

$$au + bv = a'du + b'dv = d(a'u + b'v) = \text{PGCD}(a, b).$$

Exemple

Avec $a = 55$ et $b = 5$

Correction

Le PGCD de $a = 5$ et $b = 55$ est $d = 5$ et on a par exemple :

$$(-10)a + b = 5$$

Remarque

Attention ! Le couple $(u; v)$ n'est pas unique. Trouver deux couples $(u\ ;\ v)$ pour $a = 3$ et $b = 2$.

Correction

Le PGCD de $a = 3$ et $b = 2$ est $d = 1$ et on a par exemple :

- $1a - 1b = 1$ donc le couple $(1\ ;\ -1)$ convient;
- $3a - 4b = 1$ donc le couple $(3\ ;\ -4)$ convient;

Remarque

Attention encore ! La réciproque de l'identité de Bézout est fausse.
Utiliser l'égalité $3 \times 2 + 2 \times (-2) = 2$ pour vous en convaincre.

Exercice 8

Déterminer le PGCD d de 235 et 45 puis des coefficients de Bézout associés.

Correction

1. Le PGCD de 235 et 45 est 5 donc il existe des entiers u et v tels que :

$$235u + 45v = 5$$

2. Pour les déterminer, on peut se ramener à l'équation diophantienne :

$$47u + 9v = 1$$

Par divisions euclidiennes successives on obtient avec $a = 47$ et $b = 9$:

Division euclidienne	**Reste**	**Egalité avec a et b**
$47 = 9 \times 5 + 2$	$2 = 47 - 5 \times 9$	$2 = a - 5\,b$
$9 = 2 \times 4 + 1$	$1 = 9 - 4 \times 2$	$1 = b - 4 \times (a - 5\,b)$ $1 = -4\,a + 21\,b$

Le PGCD des nombres 47 et 9 est le dernier reste non nul du procédé, c'est-à-dire 1.
Les nombres 47 et 9 sont donc premiers entre eux et le théorème 1 dit de Bézout-Bachet assure donc l'existence de couples $(u\,;\,v)$ d'entiers relatifs solutions de l'équation :

$$47\,u + 9\,v = 1$$

Pour trouver une solution, il suffisait d'exprimer le reste de la division euclidienne en fonction de a et b pour chaque ligne du procédé. Un couple solution de l'équation $47\,u + 9\,v = 1$ est donc :

$$\boxed{(u = -4\,;\,v = 21)}$$

Propriété 10

Soient a, b et c trois entiers tels que a et b ne soient pas simultanément nuls.
L'équation

$$ax + by = c$$

admet des couples d'entiers (x, y) solutions si, et seulement si, le nombre c est un multiple de PGCD(a, b).

Preuve

1. **Montrer que si l'équation $ax + by = c$ admet des solutions, alors PGCD$(a, b) \mid c$.**
   On pose $d = \text{PGCD}(a, b)$. Il existe deux entiers a' et b' tels que $a = da'$ et $b = db'$. Soit maintenant (x, y) un couple d'entiers solution de l'équation $ax + by = c$. Alors on peut réécrire cette égalité comme suit :

   $$da'x + db'y = c,$$

   autrement dit,

   $$d(a'x + b'y) = c.$$

   Ainsi, $d \mid c$.
2. **Réciproquement, supposons que c est un multiple de PGCD(a, b).**
   Soit c' l'entier tel que $c = c' \cdot \text{PGCD}(a, b)$. Déduisons de l'identité de Bézout qu'il existe un couple solution de l'équation $ax + by = c$.
   D'après l'identité de Bézout, il existe deux entiers x et y tels que :

   $$ax + by = \text{PGCD}(a, b).$$

   En multipliant les deux membres de l'égalité par c', on obtient alors :

   $$a(c'x) + b(c'y) = c.$$

   Le couple d'entiers $(c'x, c'y)$ est donc solution de l'équation $ax + by = c$.

Exemple

1. L'équation $12x + 4y = 32$ admet des couples d'entiers (x, y) parmi ses solutions car PGCD$(12, 4) = 4$ et $4 \mid 32$.
2. L'équation $2x + 6y = 3$ n'admet pas de couples de solutions entières car PGCD$(2, 6) = 2$ et $2 \nmid 3$.

VI. Théorème de Gauss

VI.1 Le théorème du Gauss

Théorème 2 (Carl Friedrich Gauss, 1777-1855)

Soit a, b, c des entiers.

Si $\begin{cases} a \text{ divise le produit } bc \\ a \text{ et } b \text{ sont premiers entre eux} \end{cases}$, alors a divise c.

Ce que l'on peut écrire :

$$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \Longrightarrow a \mid c$$

Remarque : Le mathématicien allemand Carl Friedrich Gauss énonce et prouve ce théorème (sous forme de lemme en fait) en 1801 dans son ouvrage « *Disquisitiones arithmeticae* ».

Preuve

Supposons que a divise bc et que a et b soient premiers entre eux.
Alors, PGCD$(a, b) = 1$.
D'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que :

$$au + bv = 1.$$

En multipliant cette égalité par c, on obtient :

$$auc + bvc = c.$$

Or, par hypothèse, $a \mid bc$ et il est clair que $a \mid auc$. On en déduit que :

$$a \mid (auc + bvc).$$

Ainsi, $a \mid c$.

VI.2 Une conséquence du théorème

Propriété 11

a, b et c sont trois entiers relatifs non nuls.
Si b et c sont premiers entre eux **et si** b et c divisent a, **alors** bc divise a.
Ce que l'on peut écrire :

$$\begin{cases} b \mid a \text{ et } c \mid a \\ b \wedge c = 1 \end{cases} \Longrightarrow bc \mid a$$

Preuve

Soient b et c deux diviseurs de a premiers entre eux, et soient b' et c' les entiers tels que $bb' = a$ et $cc' = a$. On a donc :

$$bb' = cc'.$$

Ainsi, $b \mid cc'$. Comme b et c sont premiers entre eux, alors, d'après le théorème de Gauss, b divise c'.
Il existe donc un entier m tel que :

$$c' = bm.$$

On en déduit :

$$a = cc' = cbm.$$

D'où bc divise a.

VI.3 Application : Équation Diophantienne

Exercice 9

Déterminer TOUS les entiers u et v tels que $6u + 11v = 1$

Correction

- Une solution particulière.
Par divisions euclidiennes successives on obtient avec $a = 11$ et $b = 6$:

Division euclidienne	**Reste**	**Egalité avec a et b**
$11 = 6 \times 1 + 5$	$5 = 11 - 1 \times 6$	$5 = a - 1\,b$
$6 = 5 \times 1 + 1$	$1 = 6 - 1 \times 5$	$1 = b - 1 \times (a - 1\,b)$ $1 = -1\,a + 2\,b$

Le PGCD des nombres 11 et 6 est le dernier reste non nul du procédé, c'est-à-dire 1.
Les nombres 11 et 6 sont donc premiers entre eux et le théorème 1 dit de Bézout-Bachet assure donc l'existence de couples $(u\,;\,v)$ d'entiers relatifs solutions de l'équation :

$$6\,u + 11\,v = 1$$

Pour trouver une solution, il suffisait d'exprimer le reste de la division euclidienne en fonction de a et b pour chaque ligne du procédé. Un couple solution de l'équation $6\,u + 11\,v = 1$ est donc :

$$\boxed{(u = 2\,;\,v = -1)}$$

- Solutions générales.

  - Transformation de l'équation
  Puisque le couple $(2\,;\,-1)$ est une solution particulière de l'équation (E) on a : $6 \times 2 + 11 \times (-1) = 1$.
  Donc
  $$\begin{cases} 6 \times u + 11 \times v = 1 \\ 6 \times 2 + 11 \times (-1) = 1 \end{cases} \underset{\text{par soustraction}}{\Longrightarrow} 6(u-2) + 11(v+1) = 0$$
  Donc l'équation (E) devient :
  $$(E) \quad : \quad 6(u-2) = 11(-v-1)$$

  - Application du théorème de Gauss

Théorème 3 (Carl Friedrich Gauss, 1777-1855)

Soit a, b, c des entiers.

$$\boxed{\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \Longrightarrow a \mid c}$$

Remarque : Le mathématicien allemand Carl Friedrich Gauss énonce et prouve ce théorème (sous forme de lemme en fait) en 1801 dans son ouvrage « *Disquisitiones arithmeticae* ».

$$(E) \quad : \quad 6(u-2) = 11(-v-1)$$

Puisque 6 et 11 sont premiers entre eux, alors en appliquant le théorème de Gauss, l'entier 6 divise $(-v-1)$ et 11 divise $(u+1)$.
Il existe donc des entiers k et k' tels que :

$$\begin{cases} -v-1 &= 6k \\ u-2 &= 11k' \end{cases}$$

En reportant dans l'équation (E) on obtient

$$6 \times 11k' = 11 \times 6k \iff k = k'$$

Ainsi, les solutions de l'équation (E) sont les couples de la forme

$$\boxed{\left(2+11k \ ; \ -1-6k\right) \ ; \ k \in \mathbb{Z}}$$

Fin du cours