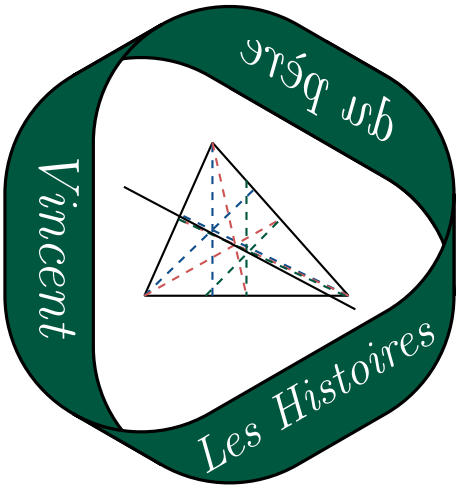
Lycée Lucie Aubrac - Terminale



Chapitre 5
Arithmétique
PGCD et applications

Table des matières

1 PGCD **2**
1.1 Définitions et premières propriétés . . . 2
1.2 Algorithme d'Euclide . . . 2
1.3 Corollaires de l'algorithme d'Euclide . . . 4

2 Identité et théorème de Bézout **5**
2.1 Identité de Bézout . . . 5
2.2 Théorème de Bézout . . . 7

3 Théorème de Gauss et corollaire **7**
3.1 Théorème de Gauss . . . 7
3.2 Corollaire du théorème de Gauss . . . 8

4 Applications **9**
4.1 Études de divisibilité . . . 9
4.2 Démonstration de l'irrationalité de $\sqrt{2}$ . . . 9
4.3 Détermination d'un inverse modulo n . . . 11
4.4 Résolution d'équations diophantiennes . . . 12
4.4.1 Résolution d'équations de la forme $ax = by$ . . . 12
4.4.2 Résolution d'équations de la forme $ax + by = k$ . . . 13

1 PGCD

1.1 Définitions et premières propriétés

Définition 1

Soient a, $b \in \mathbb{Z}$ tels que $(a;b) \neq (0,0)$.
L'ensemble des diviseurs communs à a et à b admet un plus grand élément appelé **Plus Grand Commun Diviseur de a et b**, noté $\text{PGCD}(a\,;b)$.

Démonstration.
L'ensemble des diviseurs communs à a et à b admet un plus grand élément car cet ensemble est inclus dans $\mathbb{Z}$, est non vide (il contient 1) et est majoré par $\max(|a|\,;|b|)$. □

Exemples.

- $\text{PGCD}(6\,;10) = 2$
- Pour tout $a \in \mathbb{N}$, $\text{PGCD}(a\,;1) = 1$ et $\text{PGCD}(a\,;0) = a$.

Proposition 1

Soient a, $b \in \mathbb{Z}$ tels que $(a\,;b) \neq (0\,;0)$.

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

Proposition 2

Soient a, $b \in \mathbb{N}$ tels que $a \neq 0$.

- $\text{PGCD}(a\,;b) \geqslant 1$;
- $a|b \iff \text{PGCD}(a\,;b) = a$;

1.2 Algorithme d'Euclide

Proposition 3

Soient a, $b \in \mathbb{N}^*$ tels que $a > b$. On note q et r le quotient et le reste de la division euclidienne de a par b. Alors,

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

Démonstration.
On note E_1 l'ensemble des diviseurs communs à a et à b et E_2 l'ensemble des diviseurs communs à b et à r. On va montrer que $E_1 = E_2$.

- Supposons que $d \in E_1$, c'est-à-dire que d divise a et b.
  On sait que $a = bq + r$ donc $r = a - bq$.
  Ainsi, l'entier r est une combinaison linéaire de a et b donc r est divisible par d. Finalement, d est un diviseur de b et de r donc $d \in E_2$.

- Supposons que $d \in E_2$, c'est-à-dire que d divise b et r.
  On sait que $a = bq + r$.
  Ainsi, l'entier a est une combinaison linéaire de b et r donc a est divisible par d. Finalement, d est un diviseur de a et de b donc $d \in E_1$.

Au final, on a montré que $E_1 = E_2$. Ces deux ensembles étant égaux, ils ont nécessairement le même plus grand élément d'où $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r)$. □

Exemple.
$\text{PGCD}(512\,;20) = \text{PGCD}(20\,;12) = 4$ car le reste de la division de 512 par 20 est 12.

Proposition 4

Soient a, $b \in \mathbb{N}^*$ tels que $a > b$.
On définit par récurrence la suite d'entiers naturels $(r_n)_{n\in\mathbb{N}}$ tels que :
- r_0 est le reste de la division euclidienne de a par b.
- $\rightarrow$ Si $r_0 = 0$, on pose $r_1 = 0$;
  $\rightarrow$ Sinon r_1 est le reste de la division euclidienne de b par r_0.
- pour tout $n \geqslant 1$:
  $\rightarrow$ Si $r_n = 0$, on pose $r_{n+1} = 0$.
  $\rightarrow$ Sinon, r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n.

Alors, cette suite d'entiers est nulle à partir d'un certain rang et la dernière valeur non nulle prise par cette suite est le PGCD de a et b.

Démonstration.
- On va montrer que la suite s'annule à partir d'un certain (il est clair qu'elle sera ensuite nulle pour les rangs suivants).
  Supposons par l'absurde que pour tout n, $r_n \neq 0$. Comme pour tout $n \geqslant 1$, r_{n+1} est défini comme le reste de la division de r_{n-1} par r_n, on sait que $r_{n+1} < r_n$ et donc la suite $(r_n)_{n\in\mathbb{N}}$ est strictement décroissante. Comme il s'agit d'une suite d'entiers naturels, on en déduit qu'elle s'annule à partir d'un certain rang, ce qui est impossible par hypothèse.
  Ainsi, on a montré qu'il existe un entier n_0 tel que pour tout $n \geqslant n_0$, $r_{n_0} = 0$.
- La propriété 1.2 justifie que :

$$\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r_0) = \text{PGCD}(r_0\,;r_1) = \ldots = \text{PGCD}(r_{n_0-1}\,;r_{n_0})$$
$$= \text{PGCD}(r_{n_0-1};\,0) = r_{n_0-1} \quad \text{(qui est la dernière valeur non nulle de la suite).}$$

□

Exemple.
Déterminer le PGCD de 896 et 259.

Solution :

$$\begin{aligned} 896 &= 259 \times 3 + 119 \\ 259 &= 119 \times 2 + 21 \\ 119 &= 21 \times 5 + 14 \\ 21 &= 14 \times 1 + 7 \\ 14 &= 7 \times 2 + 0 \end{aligned}$$

Ainsi, on a $\text{PGCD}(896\,;259) = 7$.

Histoire – Algorithme d'Euclide

L'algorithme d'Euclide a été présenté dans *Les Éléments* vers l'an 300 av. J.-C. Il est présenté d'une part sous forme arithmétique mais également géométrique en cherchant à construire une unité de mesure commune à deux longueurs. A la différence de l'algorithme arithmétique, le procédé géométrique ne s'arrête pas nécessairement. Il faut en fait que le rapport des deux longueurs soit rationnel pour que l'on soit sûr que le procédé s'arrête.

Euclide

1.3 Corollaires de l'algorithme d'Euclide

Proposition 5

Pour tous a, $b \in \mathbb{N}^*$ et $d \in \mathbb{N}$:

$$d|a \text{ et } d|b \iff d|\text{PGCD}(a\,;b).$$

Démonstration.
Soient a, $b \in \mathbb{N}^*$.
Dans l'algorithme d'Euclide, r_0 est reste de la division euclidienne de a par b. D'après démonstration de la propriété 1.2, on sait que l'ensemble des diviseurs communs à a et à b est égale à l'ensemble des diviseurs communs à b et à r_0. On note E cet ensemble.
Comme r_1 est le reste de la division de r_0 par b, on en déduit que E est aussi l'ensemble des diviseurs communs de r_0 et r_1.
En procédant par récurrence, on montre finalement que E est l'ensemble des diviseurs communs de $r_{n_0-1} = \text{PGCD}(a\,;b)$ (le dernier reste non nul) et de 0, ce qui correspond à l'ensemble des diviseurs de $\text{PGCD}(a\,;b)$. □

Proposition 6

Pour tous a, $b \in \mathbb{N}$ et $k \in \mathbb{N}$,

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

Démonstration.
Pour calculer $\text{PGCD}(ka;kb)$, toutes les étapes de l'algorithme d'Euclide seront les mêmes que pour calculer $\text{PGCD}(a\,;b)$ à un facteur multiplicatif k près. □

Définition 2

Soient a, $b \in \mathbb{N}$ et $k \in \mathbb{Z}^*$.
On dit que a et b sont premiers entre eux lorsque $\text{PGCD}(a\,;b) = 1$.

Proposition 7

Soient a, $b \in \mathbb{N}^*$ et avec $d = \text{PGCD}(a\,;b)$.

Il existe des entiers premiers entre eux a' et b' tels que $\begin{cases} a = da' \\ b = db' \end{cases}$

Démonstration.
Soient a, $b \in \mathbb{N}^*$ et $k \in \mathbb{Z}^*$ avec $d = \text{PGCD}(a;b)$. Comme d est un diviseur commun de a et b, il existe a' et b' des entiers tels que $a = da'$ et $b = db'$. Il suffit donc de montrer que a' et b' sont premiers entre eux. Or, on a :

$$\begin{aligned} \text{PGCD}(a;b) &= \text{PGCD}(da'\,;db') \\ &= d \times \text{PGCD}(a'\,;b') \end{aligned}$$

Ainsi, $d = d \times \text{PGCD}(a'\,;b')$ et comme $d \neq 0$ (a et b sont non nuls simultanément), on en déduit que $\text{PGCD}(a'\,;b') = 1$. □

2 Identité et théorème de Bézout

2.1 Identité de Bézout

Proposition 8 – Identité de Bézout

Soient a, $b \in \mathbb{N}^*$.

Il existe des entiers relatifs u et v tels que

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

Démonstration.
On considère la suite des divisions de l'algorithme d'Euclide (où r_{n_0-1} est le dernier reste non nul, c'est-à-dire $r_{n_0-1} = \text{PGCD}(a\,;b)$) :

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0q_1 + r_1 \\ &\vdots \quad \vdots \\ r_{k-1} &= r_kq_{k+1} + r_{k+1} \\ &\vdots \quad \vdots \\ r_{n_0-4} &= r_{n_0-3}q_{n_0-2} + r_{n_0-2} \\ r_{n_0-3} &= r_{n_0-2}q_{n_0-1} + r_{n_0-1} \\ r_{n_0-2} &= r_{n_0-1}q_{n_0} + 0 \end{aligned}$$

L'avant dernière égalité donne :

$$\text{PGCD}(a\,;b) = r_{n_0-1} = r_{n_0-3} - r_{n_0-2}q_{n_0-1} \quad (*)$$

Cela signifie que PGCD$(a\,;b)$ est une combinaison linéaire de r_{n_0-3} et r_{n_0-2}. En exprimant r_{n_0-2} dans la ligne du dessus et en la réinjectant dans l'égalité (*), on obtient ensuite :

$$\begin{aligned}\text{PGCD}(a\,;b) &= r_{n_0-3} - (r_{n_0-4} - r_{n_0-3}q_{n_0-2})q_{n_0-1}\\ &= r_{n_0-3}(1+q_{n_0-2}) - r_{n_0-4}\end{aligned}$$

Cela signifie que PGCD$(a\,;b)$ est une combinaison linéaire de r_{n_0-4} et r_{n_0-3}. De proche en proche, on pourra finalement écrire PGCD$(a\,;b)$ comme une combinaison linéaire de a et b. □

Exemple.
On sait que PGCD$(896\,;259) = 7$. Déterminer des entiers relatifs u et v tels que $896u+259v = 7$.
Solution :
On écrit les différentes étapes de l'algorithme d'Euclide :

$$\begin{aligned}896 &= 259\times 3 + 119\\ 259 &= 119\times 2 + 21\\ 119 &= 21\times 5 + 14\\ 21 &= 14\times 1 + 7\end{aligned}$$

En remontant l'algorithme, on obtient :

$$\begin{aligned}7 &= 21 - 14\times 1\\ &= 21 - (119 - 21\times 5)\times 1\\ &= 6\times 21 - 119\\ &= 6\times(259 - 119\times 2) - 119\\ &= 6\times 259 - 13\times 119\\ &= 6\times 259 - 13\times(896 - 259\times 3)\\ &= -13\times 896 + 45\times 259\end{aligned}$$

Ainsi, $896u + 259v = 7$ avec $u = -13$ et $v = 45$.

Méthode – Déterminer une identité de Bézout avec deux entiers a et b

- Effectuer l'algorithme d'Euclide.
- Remonter les lignes de l'algorithme d'Euclide pour écrire PGCD$(a;b)$ comme une combinaison linéaire des restes jusqu'à obtenir une combinaison linéaire de a et b.

Histoire – Identité de Bézout

L'identité de Bézout porte le nom du mathématicien français **Étienne Bézout** (1730-1783). Ce résultat avait cependant déjà été découvert et démontré par **Claude Gaspard Bachet de Méziriac** (1581-1638). Bézout a en fait généralisé un résultat similaire pour les polynômes. Pour cette raison, l'identité de Bézout prend parfois le nom de « théorème de Bachet-Bézout ».

Étienne Bézout

2.2 Théorème de Bézout

Proposition 9 – Théorème de Bézout

Soient a, $b \in \mathbb{Z}^*$. Les entiers a et b sont premiers entre eux si, et seulement si, il existe des entiers relatifs u et v tels que

$$au + bv = 1.$$

Démonstration.

- Supposons que $\text{PGCD}(a\,;b) = 1$. D'après l'identité de Bézout, il est immédiat de voir qu'il existe des entiers relatifs u et v tels que $au + bv = \text{PGCD}(a\,;b) = 1$.
- Réciproquement, supposons qu'il existe des entiers relatifs u et v tels que $au + bv = 1$. Soit d un diviseur commun de a et b. On en déduit que d divise la combinaison linéaire $au + bv$ donc d divise 1. Ainsi, on en déduit que $d = 1$ qui est le seul diviseur commun de a et b.
  Par conséquent, $\text{PGCD}(a\,;b) = 1$.

□

Remarque.

- L'équivalence n'est vraie que si $\text{PGCD}(a\,;b) = 1$.
  Dans le cas général, seule l'identité de Bézout est vraie.
- Le couple $(u; v)$ de l'identité de Bézout n'est pas unique.

3 Théorème de Gauss et corollaire

3.1 Théorème de Gauss

Proposition 10 – Théorème de Gauss

Soient a, b, $c \in \mathbb{Z}^*$.
Si $a|bc$ et si a et b sont premiers entre eux, alors $a|c$.

Démonstration.
Soient a, b, $c \in \mathbb{Z}^*$ tels que $a|bc$ et tels que a et b sont premiers entre eux.
a et b sont premiers entre eux donc, d'après le théorème de Bézout, il existe des entiers u et v tels que $au + bv = 1$. Ainsi, en multipliant par c, on obtient :

$$auc + bvc = c.$$

Comme $a|a$ et $a|bc$, on en déduit que a divise la combinaison linéaire $auc + bcv$, c'est-à-dire $a|c$. □

Remarque.
La condition « a et b sont premiers entre eux » est indispensable.
En effet, 9 divise $6 \times 15 = 90$ et pourtant 9 ne divise ni 6, ni 15.

Histoire – Théorème de Gauss

Carl Friedrich Gauß (1777-1855) est l'un des mathématiciens les plus célèbres du XIX^e siècle. On le surnomme « le prince des mathématiques » et il existe un nombre important de résultats qui portent son nom. Il a démontré le théorème ci-dessus en 1801 dans un ouvrage intitulé *Diquisitiones arithmeticae*. C'est d'ailleurs la même année qu'il a déterminé la trajectoire de la planète naine *Cérès* en utilisant notamment la méthode des moindres carrés.

Carl Friedrich Gauß

3.2 Corollaire du théorème de Gauss

Proposition 11 – (Corollaire)

Soient a, b, $c \in \mathbb{Z}^*$ tels que $b|a$, $c|a$ et tels que $\text{PGCD}(b\,;c) = 1$, alors $bc|a$.

Démonstration.
Soient a, b, $c \in \mathbb{Z}^*$ tels que $b|a$, $c|a$ et tels que $\text{PGCD}(b\,;c) = 1$.
Comme $b|a$ et $c|a$, il existe des entiers k et l tels que $a = bk = cl$. Ainsi, $c|bk$.
Mais comme b et c sont premiers entre eux, on en déduit d'après le théorème de Gauss que $c|k$.
Donc il existe un entier k' tel que $k = ck'$.
Finalement, on obtient $a = b(ck') = bck'$ donc $bc|a$. □

La propriété précédente se reformule à l'aide de congruences de la façon suivante :

Proposition 12 – (Corollaire)

Soient a, b, $c \in \mathbb{Z}^*$.

$$\begin{cases} a \equiv 0\,[b] \\ a \equiv 0\,[c] \\ \text{PGCD}(b\,;c) = 1 \end{cases} \implies a \equiv 0\,[bc]\,.$$

4 Applications

4.1 Études de divisibilité

Exemple.
Soit $p \geqslant 5$ un nombre premier. Montrer que $p^2 - 1$ est divisible par 24.

Solution :
Comme $24 = 8 \times 3$, on commence par montrer que $p^2 - 1$ est divisible par 8 et par 3.

- En raisonnant modulo 8 (on sait que p est impair) :

p [8]	0	1	2	3	4	5	6	7
$p^2 - 1$ [8]	×	0	×	0	×	0	×	0

  Ainsi, cela prouve que pour tout $p \geqslant 5$ premier, $8|p^2 - 1$.
- En raisonnant modulo 3 :

p [3]	0	1	2
$p^2 - 1$ [3]	×	0	0

  Ainsi, cela prouve que pour tout $p \geqslant 5$, $3|p^2 - 1$.
- Finalement, on a prouvé que pour tout nombre premier $p \geqslant 5$, $3|p^2 - 1$ et $8|p^2 - 1$. D'après le théorème de Gauss (son corollaire), comme $\text{PGCD}(8\,;3) = 1$, on en déduit que $24|p^2 - 1$.

Méthode – Établir une relation de divisibilité par n

- Décomposer n comme un produit de facteurs premiers entre eux.
- Montrer que la quantité considérée est divisible par chacun des facteurs.
- Utiliser le théorème de Gauss (corollaire).

4.2 Démonstration de l'irrationalité de $\sqrt{2}$

Histoire – Crise des irrationnels

La découverte de l'irrationalité de $\sqrt{2}$ a provoqué une véritable crise dans les mathématiques grecques. À l'époque, les mathématiciens considéraient en effet que le monde physique peut se comprendre à travers des rapports de longueurs entières. Une légende dit même que le mathématicien **Hippase de Métaponte** (500 av. J.-C.) qui a découvert le caractère « incommensurable » (irrationnel) de $\sqrt{2}$ a été condamné à la noyade par ses condisciples. Si cela n'est pas du tout assuré historiquement, il n'en reste pas moins que cette histoire traduit les difficultés qu'ont eu les grecs à accepter l'existence de nombres irrationnels.

Hippase de Métaponte

Proposition 13 – (Lemme)

Soit $a \in \mathbb{Z}$. Alors,
- a est pair $\iff a^2$ est pair.
- a est impair $\iff a^2$ est impair.

Démonstration.
Soit $a \in \mathbb{Z}$.
- On suppose que a est pair.
  Il existe $k \in \mathbb{Z}$ tel que $a = 2k$.
  Donc $a^2 = (2k)^2 = 4k^2 = 2 \times 2k^2$.
  On pose $k' = 2k^2$.
  On a donc $a^2 = 2k'$, ce qui signifie que a^2 est pair.
- On suppose que a est impair.
  Il existe $k \in \mathbb{Z}$ tel que $a = 2k + 1$.
  Donc $a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2 \times (2k^2 + 2k) + 1$.
  On pose $k' = 2k^2 + 2k$.
  On a donc $a^2 = 2k' + 1$, ce qui signifie que a^2 est impair.
- On suppose que a^2 est pair.
  On souhaite montrer que a est nécessairement pair.
  En fait, si a était impair, on a montré que a^2 serait impair, ce qui serait absurde.
- On raisonne de même pour montrer que si a^2 est impair, alors a est impair.

□

Proposition 14

Le nombre réel $\sqrt{2}$ est irrationnel.

Démonstration.
On suppose par l'absurde qu'il existe deux entiers a et b premiers entre eux (avec $b \neq 0$) tels que $\sqrt{2} = \dfrac{a}{b}$.
Ainsi, en élevant cette égalité au carré, on obtient :

$$2 = \frac{a^2}{b^2}.$$

Donc $a^2 = 2b^2$ (*)
Cela signifie que a^2 est pair et donc que a est pair d'après le lemme précédent (propriété 4.2).
Ainsi, il existe $k \in \mathbb{Z}$ tel que $a = 2k$.
En réinjectant dans l'égalité (*), on obtient : $4k^2 = 2b^2$ donc $2k^2 = b^2$.
Cela signifie que b^2 est pair et donc que b est pair d'après le lemme précédent.
Finalement, a et b sont tous les deux pairs, ce qui est absurde car ils ont été supposés premiers entre eux. □

4.3 Détermination d'un inverse modulo n

Proposition 15

Soint $n \geqslant 2$. Alors $a \in \mathbb{N}$ est inversible modulo n si, et seulement si, $\text{PGCD}(a\,;n) = 1$.

Démonstration.
Soit $n \geqslant 2$ et $a \in \mathbb{N}$. Alors,
$\text{PGCD}(a\,;n) = 1$
$\iff$ il existe u, $v \in \mathbb{Z}$ tels que $au + nv = 1$
$\iff$ il existe u, $v \in \mathbb{Z}$ tels que $1 - au = nv$
$\iff$ il existe $u \in \mathbb{Z}$ tel que $n|1 - au$
$\iff$ il existe $u \in \mathbb{Z}$ tel que $1 - au \equiv 0\,[n]$
$\iff$ il existe $u \in \mathbb{Z}$ tel que $au \equiv 1\,[n]$. □

Exemple.
Montrer que 13 est inversible modulo 36 et déterminer son inverse.

Solution :
On effectue l'algorithme d'Euclide :

$$\begin{aligned} 36 &= 13 \times 2 + 10 \\ 13 &= 10 \times 1 + 3 \\ 10 &= 3 \times 3 + 1 \end{aligned}$$

Ainsi, $\text{PGCD}(13\,;36) = 1$ donc 13 est bien inversible modulo 36.
Par ailleurs, en remontant l'algorithme d'Euclide :

$$\begin{aligned} 1 &= 10 - 3 \times 3 \\ &= 10 - (13 - 10 \times 1) \times 3 \\ &= 4 \times 10 - 3 \times 13 \\ &= 4 \times (36 - 13 \times 2) - 3 \times 13 \\ &= 4 \times 36 - 11 \times 13 \end{aligned}$$

Ainsi, en considérant la dernière égalité modulo 36, on voit que $-11 \times 13 = 1\,[36]$.
Cela signifie donc que l'inverse de 13 est -11, soit 25 modulo 36.

Méthode – Déterminer l'inverse de a modulo n

- Déterminer une identité de Bézout entre a et n :

$$au + nv = 1$$

- Considérer l'égalité modulo n.

4.4 Résolution d'équations diophantiennes

On appelle **équation diophantienne** une équation à coefficients entiers pour laquelle on cherche les solutions entières.

Histoire – Équations diophantiennes

Mathématicien grec de l'antiquité, **Diophante** est l'auteur d'*Arithmetica* dans lequel il résout certaines équations où les inconnues sont des entiers. Par la suite, de nombreux mathématiciens se sont intéressés à ce genre d'équations. En général, l'équation posée correspond à un problème facilement compréhensible mais qui peut être très difficile à résoudre. Á noter que la plupart du temps, les équations diophantiennes n'ont pas d'application immédiate, en physique par exemple. Elles ont cependant poussé les mathématiciens à développer de nouvelles théories au cours de l'histoire. L'exemple du grand théorème de Fermat qui a été conjecturé par **Pierre de Fermat** au XVII^{e} siècle et démontré plus de trois siècles plus tard par **Andrew Wiles** en 1994 en est un exemple frappant. Ce théorème énonce que pour tout $n \geqslant 3$, il n'existe pas de triplet d'entiers non nuls $(x\,;y\,;z)$ tels que $x^n + y^n = z^n$.

Édition de 1621 de *Arithmetica*

4.4.1 Résolution d'équations de la forme $ax = by$

Exemple.
Résoudre dans $\mathbb{Z}^2$ l'équation (E) : $36x = 45y$.

Solution.
On a PGCD$(36; 45) = 9$.
On simplifie par l'équation en divisant par 9 :

$$36x = 45y \iff 4x = 5y.$$

Analyse : Supposons que $(x; y)$ est une solution de l'équation (E).
Alors $4x = 5y$ donc, d'après le théorème de Gauss, comme 4 et 5 sont premiers entre eux, on en déduit que $4|y$.
Ainsi, il existe $k \in \mathbb{Z}$ tel que $y = 4k$.
Par la suite, on en déduit que $4x = 5 \times (4k)$ et donc que $x = 5k$.
Synthèse : Pour tout $k \in \mathbb{Z}$, le couple $(5k\,;4k)$ est une solution de (E).
Finalement, on a montré que $\mathcal{S} = \big\{(5k\,;4k), k \in \mathbb{Z}\big\}$.

Méthode – Résoudre une équation de la forme $ax = by$

- Simplifier en divisant l'équation par PGCD$(a\,;b)$
- Procéder par analyse / synthèse en utilisant le théorème de Gauss.

4.4.2 Résolution d'équations de la forme $ax + by = k$

Proposition 16

Soient a, $b \in \mathbb{Z}^*$ et $k \in \mathbb{Z}^*$.
L'équation $ax + by = k$ (d'inconnues x et y) admet des solutions entières si, et seulement si, $\text{PGCD}(a\,;b) \mid k$.

Démonstration.

- Supposons que l'équation $ax + by = k$ admette une solution. Cela signifie qu'il existe des entiers x_0 et y_0 tels que $ax_0 + by_0 = k$. Comme $\text{PGCD}(a\,;b)$ est un diviseur commun de a et b, il divise toute combinaison linéaire de a et b. En particulier, $\text{PGCD}(a\,;b)$ divise $ax_0 + by_0 = k$.
- Réciproquement, supposons que $\text{PGCD}(a;b)|k$. Cela signifie qu'il existe $k' \in \mathbb{Z}$ tel que $k = \text{PGCD}(a;b) \times k'$. Or, d'après l'identité de Bézout, il existe des entiers u_0 et v_0 tels que $au_0 + bv_0 = \text{PGCD}(a\,;b)$. En multipliant cette égalité par k', il vient :

$$au_0k' + bv_0k' = \text{PGCD}(a;b) \times k'.$$

On pose $x_0 = u_0k'$ et $y_0 = v_0k'$. Il est alors clair que le couple $(x_0\,;y_0)$ est solution de l'équation $ax + by = k$.

□

Exemple.
Déterminer l'ensemble des couples solutions des équations suivantes :

1. $15x + 33y = 7$
2. $14x + 32y = 8$.

Solution :

1. $\text{PGCD}(15, 33) = 3$. Comme 3 ne divise pas 7, l'équation n'admet aucune solution.
   En effet, si $(x;y)$ était un couple solution, on aurait $15x + 33y = 7$. Comme 3 divise 15 et 33, il faudrait qu'il divise 7, ce qui n'est pas le cas.

2. On détermine le PGCD de 14 et 32 avec l'algorithme d'Euclide.

$$\begin{aligned} 32 &= 14 \times 2 + 4 \\ 14 &= 4 \times 3 + 2 \\ 4 &= 2 \times 2 + 0 \end{aligned}$$

   Ainsi, $\text{PGCD}(14\,;32) = 2$ et comme 2 divise 8 l'équation admet des solutions.
   En remontant l'algorithme d'Euclide, il vient :

$$\begin{aligned} 2 &= 14 - 4 \times 3 \\ &= 14 - (32 - 14 \times 2) \times 3 \\ &= -3 \times 32 + 7 \times 14 \end{aligned}$$

Ainsi, en multipliant la dernière égalité par 4, il vient

$$8 = -12 \times 32 + 28 \times 14.$$

En posant, $x_0 = 28$ et $y_0 = -12$, on voit que le couple $(x_0; y_0)$ est une solution de l'équation. Soit $(x, y) \in (\mathbb{Z}^*)^2$:

$$\begin{aligned} 14x + 32y = 8 &\iff 14x + 32y = 14x_0 + 32y_0 \\ &\iff 14(x - x_0) = 32(y_0 - y) \\ &\iff 7(x - x_0) = 16(y_0 - y) \end{aligned}$$

Analyse : Supposons que x et y sont solutions.
Alors, d'après le théorème de Gauss, $7 | y_0 - y$ (car PGCD$(7\,;16) = 1$).
Donc il existe $k \in \mathbb{Z}$ tel que $y_0 - y = 7k$, c'est-à-dire $y = y_0 - 7k = -12 - 7k$.
En réinjectant cette expression dans l'égalité (*), on obtient : $7(x - x_0) = 16 \times 7k$.
Ainsi, $x - x_0 = 16k$, c'est-à-dire $x = x_0 + 16k = 28 + 16k$.

Synthèse : Si on pose $x = 28 + 16k$ et $y = -12 - 7k$ (avec $k \in \mathbb{Z}$), il est immédiat de vérifier que le couple $(x; y)$ est bien une solution de l'équation.

Finalement, $\mathcal{S} = \left\{ (28 + 16k\,; -12 - 7k)\,, k \in \mathbb{Z} \right\}$

Méthode – Résoudre une équation diophantienne de la forme $ax + by = k$

- Effectuer l'algorithme d'Euclide pour déterminer PGCD$(a\,;b)$
- Remonter l'algorithme afin de trouver une solution particulière $(x_0\,;y_0)$.
- Ecrire qu'un couple $(x\,;y)$ est solution $\iff ax + by = ax_0 + by_0$.
- Passer les x du même côté et les y du même côté puis conclure avec Gauss.

Savoir-faire du chapitre

- Déterminer le PGCD de deux entiers avec l'algorithme d'Euclide.
- Déterminer une relation de Bézout entre deux entiers.
- Connaître et utiliser les théorèmes de Bézout et de Gauss.
- Étudier une relation de divisibilité.
- Démontrer l'irrationalité de $\sqrt{2}$.
- Déterminer un inverse modulo n.
- Résoudre des équations diophantiennes de la forme $ax = by$.
- Résoudre des équations diophantiennes de la forme $ax + by = k$.

QCM d'entrainement