PGCD et théorème de Bézout

Capacités attendues en fin de chapitre :

- PGCD de deux entiers. Algorithme d'Euclide
- Établir et utiliser des tests de divisibilité, étudier la primalité de certains nombres, étudier des problèmes de chiffrement.
- Résoudre des équations diophantiennes simples.

Le mathématicien du chapitre :

Etienne Bézout (1730-1783) est un mathématicien français né à Nemours et connu pour le théorème en arithmétique qui porte son nom. Il fut examinateur des gardes de la marine. Il rédigea Le cours complet de mathématiques à l'usage de la marine et de l'artillerie qui devient plus tard le livre référence au concours d'entrée de X.

1) Diviseurs communs, PGCD

a) Déterminer les diviseurs d'un entier naturel

On détermine de tête l'ensemble des diviseurs en construisant cet ensemble par les deux « bouts ». Il suffit de chercher les diviseurs jusqu'à la racine carrée du nombre. La découverte d'un diviseur induit la découverte d'un deuxième diviseur : $48 = 16 \times 3$. L'ensemble se construit jusqu'à se rejoindre au milieu. $D(48) = \{1; 2; 3; 4; 6; 8; 12; 16; 24; 48\}$

Exemple :

Déterminer de tête l'ensemble des diviseurs des nombres ci-dessous.

$D(35) = \{1; 5; 7; 35\}$
$D(100) = \{1; 2; 4; 5; 10; 20; 25; 50; 100\}$
$D(13) = \{1; 13\}$

b) PGCD de deux entiers naturels

Puisque tous les entiers naturels sont divisibles par 1, l'ensemble des diviseurs communs à a et b est non vide et contient au moins 1.

Définition :

Soient a et b deux entiers naturels non nuls.
On note $D(a; b)$ l'ensemble des diviseurs commun à a et à b.
$D(a; b)$ contient un plus grand élément noté $PGCD(a; b)$.
On appelle le plus grand diviseur commun à a et à b

Remarques :

- $D(a; b) = D(a) \cap D(b)$
- $D(a; b)$ contient un nombre fini d'éléments car $D(a)$ et $D(b)$ possèdent un nombre fini d'éléments.
- $D(a; b) \subset D(a)$ et $D(a; b) \subset D(b)$

Exemple :

Avec les exemples ci-dessus, on a :

- $D(35; 100) = \{1; 5\}$
- $PGCD(35; 100) = 5$
- $D(35; 13) = \{1\}$
- $PGCD(35; 13) = 1$

Remarque :

Si a et b sont deux nombres entiers relatifs, alors $D(a; b) = D(|a|; \lceil b \rceil)$. On peut alors définir de la même manière $PGCD(a; b) = PGCD(|a|; \lceil b \rceil)$

c) *L'algorithme d'Euclide*

L'algorithme d'Euclide consiste à effectuer d'abord la division euclidienne de a par b puis successivement les divisions euclidiennes du diviseur et du reste de la division précédente.

Propriété :

Soient a et b deux entiers naturels non nuls et r le reste de la division euclidienne de a par b, alors $D(a;b) = D(b;r)$

Exemple :

Avec l'exemple précédent, $D(100;35) = D(35;30)$ car $100 = 2 \times 35 + 30$.
On peut aussi réitérer ce processus par transitivité. Ainsi $35 = 1 \times 30 + 5$.
On a donc $D(35;30) = D(30;5)$ soit au final $D(100;35) = D(30;5)$
On observe une rapide descente des nombres à étudier…

Méthode :

Étape	Division	Dividende	Diviseur	Reste
1	$a = b \times q_1 + r_1$	a	b	$0 \leq r_1 < b$
2	$b = r_1 \times q_2 + r_2$	b	r_1	$0 \leq r_2 < r_1$
3	$r_1 = r_2 \times q_3 + r_3$	r_1	r_2	$0 \leq r_3 < r_2$
…	…	…	…	…
n	$r_{n-2} = r_{n-1} \times q_n + 0$	r_{n-2}	r_{n-1}	0

Après avoir effectué un nombre fini de n étapes, on obtient une division euclidienne dont le reste est nul. Le $PGCD(a;b)$ est le dernier reste non nul soit $PGCD(a;b) = r_{n-1}$

Avec du python :

On peut coder de manière très simple en langage python l'algorithme d'Euclide. L'instruction while b fait tourner la boucle tant que b n'est pas nul.

```
1  def pgcd(a,b):
2      while b:
3          a,b = b,a%b
4      return(a)
```

```
> pgcd(20,50)
10
> pgcd(13,25)
1
```

Exercice :

Déterminer à la main le $PGCD(1551;132)$

Solution :

Il s'agit d'écrire en ligne toutes les divisions euclidiennes jusqu'à l'obtention d'un reste nul.
$1551 = 11 \times 132 + 99$.
$132 = 1 \times 99 + 33$
$99 = 3 \times 33 + 0$
Ainsi, $PGCD(1551;132) = 33$

Propriété :

Soient a et b deux entiers naturels non nuls et $d = PGCD(a;b)$.
L'ensemble des diviseurs communs à a et b vérifie : $D(a;b) = D(d)$

Exemple :

Avec l'exemple numérique ci-dessus :
$D(1551;132) = D(33) = \{-33, -11, -3, -1, 1, 3, 11, 33\}$

Exercice :

Pour tout entier naturel n, on donne $a = 5n + 7$ et $b = n + 1$.
Montrer que $D(a\,;b) = D(n+1\,;2)$. En déduire $PGCD(a\,;b)$ en fonction de n.

Solution :

On écrit la division euclidienne de a par b : $5n + 7 = 5(n+1) + 2$

Puisque $0 < 2 < n + 1$, c'est bien la division euclidienne de a par b
On a donc : $D(5n + 7\,;n + 1) = D(n + 1\,;2)$
Le $PGCD(a\,;b)$ est un diviseur positif de 2 soit 1 ou 2.

- Si 2 divise $n + 1$, c'est que n est impair et $PGCD(a\,;b) = 2$.
- Si 2 ne divise pas $n + 1$, c'est que n est pair et $PGCD(a\,;b) = 1$.

2) Nombres premiers entre eux

a) Couple d'entiers premiers entre eux

Définition :

Soient a et b deux entiers naturels non nuls.
On dit que a et b sont premiers entre eux lorsque $PGCD(a; b) = 1$

Remarques :

- Deux nombres premiers sont nécessairement premiers entre eux. $PGCD(2; 5) = 1$
- Deux nombres non premiers peuvent être premiers entre eux. $PGCD(10; 63) = 1$
- Deux nombres consécutifs son nécessairement premiers entre eux. $PGCD(20; 21) = 1$

Propriété :

Soient a un entier relatif et b un entier naturel non nuls.
La fraction $\frac{a}{b}$ est irréductible si et seulement si $PGCD(a; b) = 1$

Exemple :

On souhaite simplifier la fraction $\frac{250}{675}$.
Un rapide calcul donne $PGCD(250; 675) = 25$. Ainsi $\frac{250}{675} = \frac{25\times10}{25\times27} = \frac{10}{27}$
En simplifiant par le $PGCD$, on obtient une fraction irréductible.

b) Le théorème de Bézout

Théorème :

Soient a et b deux entiers relatifs non nuls.
a et b sont premiers entre eux si et seulement s'il existe deux entiers relatifs notés u et v tels que $au + bv = 1$

Remarque :

C'est la raison pour laquelle deux entiers consécutifs sont premiers entre eux.
Par exemple, $PGCD(112; 113) = 1$ car $113 \times 1 - 112 \times 1 = 1$

Exercice :

A l'aide de l'algorithme d'Euclide, déterminer deux entiers naturels tels que $38u + 15v = 1$

Correction :

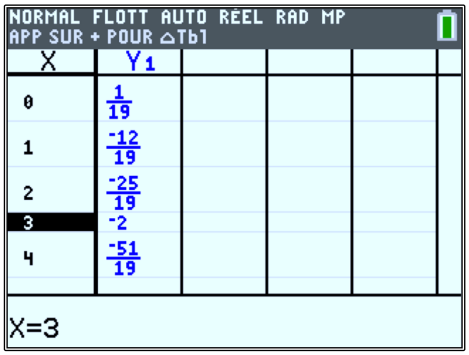
On écrit l'algorithme d'Euclide et on isole les restes non nuls obtenus.
$38 = 2 \times 15 + 8$. Soit donc $8 = 38 - 2 \times 15$
$15 = 1 \times 8 + 7$. Soit donc $7 = 15 - 1 \times 8$
$8 = 1 \times 7 + 1$. Soit donc $1 = 8 - 1 \times 7$
$7 = 7 \times 1 + 0$
On remonte alors l'algorithme d'Euclide à partir du dernier reste non nul.
$1 = 8 - 1 \times 7$
$1 = 8 - 1 \times (15 - 1 \times 8)$
$1 = 2 \times 8 - 1 \times 15$
$1 = 2 \times (38 - 2 \times 15) - 1 \times 15$
Soit au final : $1 = 2 \times 38 - 5 \times 15$. On a donc $(u; v) = (2; -5)$

Exercice :

A l'aide de la calculatrice, déterminer deux entiers relatifs tels que $13u + 19v = 1$

Solution :

On isole une des deux lettres : $13u + 19v = 1$
$\Leftrightarrow v = -\frac{13}{19}u + \frac{1}{19}$. On cherche donc les entiers u tels que $-\frac{13}{19}u + \frac{1}{19}$ donne un entier. On peut utiliser une fonction $f(x) = -\frac{13}{19}x + \frac{1}{19}$ en utilisant les valeurs entières de la table.
A l'aide de la calculatrice, on obtient $f(3) = -2$
Ainsi, $13 \times 3 + 19 \times (-2) = 1$. D'après le théorème de Bézout, on a : $PGCD(13; 19) = 1$



c) *Caractérisation du PGCD*

Théorème :

Soient a et b deux entiers relatifs non nuls.
$PGCD(a; b) = d$ si et seulement si d divise a et b et s'il existe deux entiers relatifs u et v tels que $au + bv = d$

Remarque :

La condition de divisibilité est nécessaire. On peut exhiber un contre-exemple simple.
Ainsi, $1 \times 3 + 1 \times (2) = 5$. Pourtant, 5 n'est pas le $PGCD(2; 3)$

Exercice :

Déterminer tous les couples d'entiers naturels non nuls $(x; y)$ tels que : $\begin{cases} x + y = 5664 \\ PGCD(x; y) = 354 \end{cases}$

Solution :

Le $PGCD(x; y)$ vaut 354 donc il existe un couple d'entiers $(x'; y')$ premiers entre eux tels que $x = 354x'$ et $y = 354y'$. On doit finalement résoudre $x' + y' = 16$.
On peut chercher « à la main » les couples d'entiers qui conviennent. Ils sont peu nombreux.
$(1; 15)$, $(3 ; 13)$, $(5 ; 11)$, $(7 ; 9)$.
Il y a évidemment les 4 autres couples symétriques soit au final 8 couples solutions. En multipliant par 354, on obtient :
$S = \{(354; 5310), (1062; 4602), (1770; 3894), (2478; 3186),$
$(5310; 354), (4602; 1062), (3894; 1770), (3186; 2478)\}$

3) *Conséquences du théorème de Bézout*

a) *Résolution d'équations diophantiennes*

Définition :

On appelle équation diophantienne une équation dont les inconnus sont des nombres entiers.

Théorème :

Soient a, b et c trois entiers relatifs non nuls.
L'équation $ax + by = c$ où les inconnues x et y sont des entiers relatifs admet des solutions si et seulement si c est un multiple de $PGCD(a; b)$
$PGCD(a; b) = d$ si et seulement si d divise a et b et s'il existe deux entiers relatifs u et v tels que $au + bv = d$.

Exemple :

Puisque $PGCD(12; 13) = 1$, alors l'équation $13x + 12y = 11$ admet au moins un couple d'entiers solutions.

Exercice :

On donne l'équation $39x + 42y = 2$ où x et y sont des entiers relatifs
Résoudre cette équation.

Solution :

En évaluant les diviseurs de 39 et 42, on obtient que $PGCD(39\,;42) = 3$.
Puisque 2 n'est pas un multiple de 3, cette équation ne possède aucune solution.

Python :

```
1  def bezout(a,b):
2    for u in range(-100,100):
3      for v in range(-100,100):
4        r = a*u+b*v
5        if r == 1:
6          return u,v
7    return "pas de solution"
```

On teste tous les couples d'entiers entre -100 et 100 afin de déterminer les couples solutions.

```
> bezout(39,42)
'pas de solution'
> bezout(13,19)
(-92, 63)
```

b) *Théorème de Gauss*

Théorème :

Soient a, b et c trois entiers relatifs non nuls.
Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Exemple :

5 divise 6×10 et 5 et 6 sont premiers entre eux, alors 5 divise 10.

Contre-exemple :

La condition a et b sont premiers entre eux est indispensable.
En effet 4 divise 6×2 mais 4 ne divise ni 6, ni 2.

Démonstration :

Puisque a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers relatifs notés u et v tels que $au + bv = 1$.
En multipliant les deux membres par c on obtient : $acu + bcv = c$.
a divise acu, a divise bcv car a divise bc. Par somme, a divise c

Corollaire :

Soient a, b et c trois entiers relatifs non nuls.
Si a divise c et si b divise c avec a et b sont premiers entre eux, alors ab divise c.

Exemple :

Soient n un entier naturel et $N = n(n+1)(n+2)$
Puisque n et $n+1$ sont deux entiers consécutifs, alors l'un deux est pair et 2 divise N
Puisque n , $n+1$ et $n+2$ sont trois entiers consécutifs, alors 3 divise l'un d'eux et 3 divise N. Puisque 2 et 3 sont premiers entre eux, alors 6 divise N.

Exercice :

n est un entier naturel non nul compris entre 20 et 800. On sait que la division euclidienne de n par 60 donne pour reste15 et la division euclidienne de n par 156 donne pour reste aussi 15
Déterminer l'entier n.

Solution :

On écrit les divisions euclidiennes : $n = 60b + 15$ et $n = 156b' + 15$. Ainsi $n - 15$ est divisible par 60 et par 156. Il suffit donc de trouver un multiple commun à 60 et 156 compris entre 20 et 800. On a de manière simple $156 \times 5 = 780$ et $60 \times 13 = 780$.
On a donc finalement $n = 795$

c) ***Résoudre une équation diophantienne***

On considère l'équation (E): $2x + 5y = 4$ où $(x; y) \in \mathbb{Z}^2$

Méthode :

- Trouver deux entiers relatifs u et v tels que $2u + 5v = 1$
- En déduire une solution particulière $(x_0\,;y_0)$ de (E).
- Trouver toutes les solutions de (E)

Ici, on trouve aisément $2 \times (-2) + 5 \times 1 = 1$; Dans le cas d'une équation plus compliquée, l'algorithme d'Euclide permet de trouver un couple solution. On a donc $(u\,;v) = (-2\,;1)$.
En multipliant par 4, on obtient une solution particulière de (E) :$(x_0\,;y_0) = (-8\,;4)$
On a donc $\begin{cases} 2x + 5y = 4 \\ 2x_0 + 5y_0 = 4 \end{cases}$. Soit par soustraction $2(x - x_0\,) = 5(y_0 - y)$
En remplaçant, on a alors : $2(x + 8\,) = 5(4 - y\,)$
Puisque 2 et 5 sont premiers entre eux, d'après le théorème de Gauss, 2 divise $(4 - y\,)$.
Il existe donc $k \in \mathbb{Z}$ tels que $4 - y = 2k \iff y = 4 - 2k$.
En injectant dans l'équation, on obtient, avec le même $k \in \mathbb{Z}$, $2(x + 8\,) = 5 \times 2k$
Ainsi, on obtient $x = -8 + 5k$.

Réciproquement, on vérifie que $(x\,;y) = (-8 + 5k\,;4 - 2k)$, avec $k \in \mathbb{Z}$ est solution de (E).
On remplace dans (E) : $2(-8 + 5k\,) + 5(4 - 2k\,) = -16 + 10k + 20 - 10k = 4$
Ainsi, $S = \{(-8 + 5k\,;4 - 2k)$ avec $k \in \mathbb{Z}\,\}$

d) ***Exercice sur le théorème des restes chinois***

Exercice :

Soit n un entier naturel non nul tel que : $\begin{cases} n \equiv 3[5] \\ n \equiv 2[7] \end{cases}$.
Déterminer alors toutes les solutions de ce problème.

Solution :

On écrit tout d'abord les divisions euclidiennes.
Il existe $p \in \mathbb{N}$ tel que $n = 5p + 3$
Il existe $q \in \mathbb{N}$ tel que $n = 7q + 2$
Par soustraction, on a (E): $7q - 5p = 1$
Puisque 7 et 5 sont premiers entre eux, d'après le théorème de Bézout, il existe un couple $(p\,;q) \in \mathbb{Z} \times \mathbb{Z}$ tels que $7q - 5p = 1$
(E) admet donc au moins une solution. $(p\,;q) = (4; 3)$
L'ensemble des solutions dans $\mathbb{N} \times \mathbb{N}$ est donc $S = \{(4 + 7k; 3 + 5k), k \in \mathbb{N}\}$
L'entier n s'écrit donc au final : $n = 5(4 + 7k) + 3$ avec $k \in \mathbb{N}$ soit $n = 23 + 35k$