Terminale S (Spécialité)	**Chapitre III : PGCD, Théorème de Bézout, Théorème de Gauss**	Année scolaire 2015/2016

I) PGCD de deux entiers naturels :

1) Définition :

Soient a et b, deux entiers naturels non nuls.
Posons D(a) = {ensemble des diviseurs entiers naturels de a}
D(b) = {ensemble des diviseurs entiers naturels de b}

- $D(a) \cap D(b) \neq \varnothing$: (en effet : $1 \in D(a) \cap D(b)$)
- $D(a) \cap D(b) \in \mathbb{N}$
- $D(a) \cap D(b)$ est majorée par $a \times b$

Donc $D(a) \cap D(b)$ possède un plus grand élément.
Cet élément est appelé le PGCD de a et b.

Notations : PGCD(a;b)
$D(a) \cap D(b)$ peut se noter D(a;b)

2) Calcul du PGCD. Algorithme d'Euclide.

Deux algorithmes ont déjà été étudiés au collège pour calculer le pgcd de deux entiers naturels : l'algorithme des différences et celui d'Euclide.

Algorithmes + programmes sur la calculatrice : voir en TD

3) Propriétés :

Soient a et b, deux entiers naturels non nuls :

a)

$$D(a;b) = D(a - b;b) = D(a - kb;b), \text{ pour } k \in \mathbb{N}$$

b)

$$\text{Si } k \in \mathbb{N}, \text{ PGCD}(ka;kb) = k \times \text{PGCD}(a;b)$$

$$\text{Si } k \in \mathbb{Z}, \text{ PGCD}(ka;kb) = |k| \times \text{PGCD}(a;b)$$

Exemple : $\text{PGCD}(150;100 = \text{PGCD}(3\times50;2\times50) = 50 \times \text{PGCD}(3;2) = \mathbf{50}$

c) On pose d = PGCD(a;b). Alors, il existe deux entiers naturels non nuls, a' et b', tels que :

$$\begin{cases} a = da' \\ b = db' \\ \text{PGCD}(a';b') = 1 \end{cases}$$

Démonstration : (raisonnement par double inclusion)

Montrons que D(a;b) = D(a – kb;b)

$\subseteq$: Soit $x \in D(a;b)$, alors $x|a$ et $x|b$ d'où : $x \mid a - kb$, pour $k \in \mathbb{N}$
donc : $x \in D(a - kb\ ;b)$

$\supseteq$: Soit $x \in D(a - kb\ ;b)$, alors $x \mid a - kb$ et $x \mid b$. D'où : $x \mid a - kb + kb = a$
Donc $x \in D(a;b)$

Par conséquent : $D(a;b) = D(a - kb;b)$

Conséquence : **PGCD(a;b) = PGCD(a – kb;b), pour $k \in \mathbb{N}$**

II) Théorème de Bézout :

1) Nombres premiers entre eux :

Soient a et b, deux entiers naturels non nuls.

a et b sont premiers entre eux ⇔ PGCD(a;b) = 1

2) Relation de Bézout :

Soient a et b, deux entiers naturels non nuls. On pose d = PGCD(a;b).
Alors : Il existe au moins un couple d'entiers relatifs non nuls (u;v), tels que :
$au + bv = d$

Démonstration :

Soit $E = \{x = a\times m + b\times n \in \mathbb{N}$, avec m et n, deux entiers relatifs non nuls$\}$

$E \neq \emptyset$, car $0 \in E$, en effet : en prenant $m = b \in \mathbb{Z}^*$ et $n = -a \in \mathbb{Z}^*$, on a $a \times b + b \times (-a) = 0$

On a $E \subseteq \mathbb{N}$, avec 0 le minorant de E.

E étant une partie non vide et minorée de $\mathbb{N}$: elle possède donc un plus petit élément.

Notons d, cet élément.

Par définition de E, il existe m et n, deux entiers relatifs tels que : $d = a\times m + b\times n$

Montrons que d = PGCD(a;b) :

- Tout d'abord : PGCD(a;b) | a et PGCD(a;b) | b d'où : PGCD(a;b) | $a\times m + b\times n = d$

Or, PGCD(a;b) $\in \mathbb{N}$, donc : $\underline{PGCD(a;b) \leq d}$

- Ensuite : effectuons la division euclidienne de a par d

Alors : il existe $(q;r) \in \mathbb{Z}\times\mathbb{N}$, $a = dq + r$, avec $0 \leq r < d$

Supposons $r \neq 0$:

$r = a - dq = a - (a\times m + b\times n)\times q = a\times(1 - m) + b\times(- n)q \geq 0$ d'où : $r \in E$

Or, $r < d$ et d est le plus petit élément de E.

Ce qui est contradictoire.

Donc r = 0

C'est-à-dire : $a = dq$: autrement d | a . De même, d | b. D'où : $d \in D(a;b)$

Or, PGCD(a;b) est le plus grand diviseur commun à a et à b, donc : $\underline{d \leq PGCD(a;b)}$

Finalement : $\underline{PGCD(a;b) = d}$ (CQFD)

3) Théorème :

Soient a et b, deux entiers naturels non nuls :

a et b sont premiers entre eux ⇔ il existe (u ; v) entiers relatifs tels que $au + bv = 1$

Remarques :

- C'est une équivalence. Ce qui n'est pas le cas si $au + bv = d$, avec $d \neq 1$
  Exemples : $2 = 1 + 1 = 1 \times 1 + 1 \times 1$, or $2 \neq PGCD(1;1)$

La relation $21u + 3v = 5$, avec u et v, deux entiers relatifs, ne signifie pas que 5 est le PGCD(21;3)

En effet : PGCD(21;3) = 3

- Il n'y a pas unicité du couple (u;v)

Exemple :

59 et 27 sont premiers entre eux. Déterminer un couple d'entiers relatifs (u;v) tel que :
$59u + 27v = 1$

Pour déterminer un tel couple, on « remonte » les calculs de l'algorithme d'Euclide.

On trouve : $1 = 59 \times 11 + 27 \times (- 24)$ u = 11 et v = - 24

Application :
Soit $n \in \mathbb{N}$, démontrer que $2n + 1$ et $9n + 4$ sont premiers entre eux.

Solution :
On a $9\times (2n + 1) – 2 \times (9n + 4) = 1$ ($u = 9$ et $v = - 2$)
D'après le théorème de Bézout, PGCD($2n + 1$; $9n + 4$) = 1, c'est-à-dire :
$2n + 1$ et $9n + 4$ sont premiers entre eux.

Démonstration :
- Sens direct : a et b premiers entre eux $\Leftrightarrow$ PGCD(a;b) = 1.
D'après la relation de Bézout, il existe un couple d'entiers relatifs (u;v) tel que :
$au + bv = PGCD(a;b) = 1$
- Sens réciproque : Soient a et b, deux entiers naturels non nuls.
Supposons qu'il existe un couple d'entiers relatifs avec $au + bv = 1$
Or, PGCD(a;b) | a et PGCD(a;b) | b
D'où : PGCD(a;b) | $au + bv = 1$
Donc PGCD(a;b) = 1

III) Théorème de Gauss :

(Gauss Carl-Friedrich (1777-1855) Mathématicien allemand (= « le Prince des mathématiciens »))
(Disquisitiones arithmeticae(1801))

1) Théorème :

Soient a,b et c, trois entiers tels que PGCD(a;b) = 1.
Si a| bc , alors a | c

Remarque :
L'hypothèse a et b premiers entre eux est INDISPENSABLE.
En effet : 6 | 4×3 mais 6 ∤ 4 et 6 ∤ 3

Démonstration :
a et b sont premiers entre eux $\Leftrightarrow$ $\exists (u;v) \in \mathbb{Z}^2$, $au + bv = 1$
En multipliant cette égalité par c à gauche et à droite , on a :
$acu + bcv = c$
Or, a |acu et a | bcv , d'où a divise toute combinaison linéaire à coefficients entiers de a et b.
En particulier, a | $acu + bcv = c$ Donc : **a | c**

Remarque : Il faut penser au théorème de Gauss quand on se retrouve avec une égalité de deux produits.
Exemple : Trouver tous les couples d'entiers (x;y) solutions de $5x = 3y$
(On peut bien appliquer le théorème de Gauss, car PGCD(5;3) = 1)

2) Corollaire 1 :

Soient a et b, deux entiers et p, un nombre premier tel que p | ab
alors, p | a ou p | b

Démonstration :
Supposons p, nombre premier tel que p | ab
- Soit p | a, et c'est terminé !
- Soit p ∤ a, et alors : PGCD(p;a) = 1
D'après le théorème de Gauss, p | b

3) Corollaire 2 :

Soient a, b et p, trois nombres premiers tels que p | ab alors, p = a ou p = b

Démonstration :
C'est évident à partir du corollaire 1

4) Application à la résolution des équations diophantiennes :

a) Déterminer tous les couples d'entiers (x;y) tels que 5x = 3y (E)

5 | 5x d'où : 5 | 3y
Or, PGCD(5;3) = 1
D'après le théorème de Gauss, 5 | y
C'est-à-dire : Il existe $k \in \mathbb{Z}$, y = 5k
De même, 3 | 5x avec PGCD(5;3) = 1 d'où, d'après le théorème de Gauss, 3 | x
C'est-à-dire : Il existe $k' \in \mathbb{Z}$, x = 3k'

Réciproque :
On remplace x et y par leurs expressions dans l'égalité initiale :
D'où : 5× 3k' = 3 × 5k
Donc : k = k'

Par conséquent, les solutions de l'équation (E) sont les couples suivants :
(3k;5k), avec $k \in \mathbb{Z}$}

Remarques : - Il y a une infinité de couples solutions
- Par exemple : (0;0) , (3;5) , (-6;-10), (24;40), etc... sont des couples solutions
- Graphiquement : la droite d'équation 5x -3y = 0 possède une infinité de points à coordonnées entières

b) Résolution de l'équation diophantienne : 3x + 2y = 10 (E)

Tout d'abord, PGCD(3;2) = 1 (=nombres premiers entre eux) et 1 | 10 d'où (E) possède des solutions entières.

On pose (E_0) : 3x + 2y = 1
Cette équation admet des solutions entières d'après le théorème de Bézout

(1;-1) est une solution particulière évidente de (E_0)

Remarque : Si il n'y a apparemment pas de solution particulière évidente de l'équation, il suffit de « remonter » l'algorithme d'Euclide (voir la vidéo correspondante sur le site) pour en déterminer une.

Pour obtenir une solution particulière de (E), il suffit de multiplier celle trouvée pour (E_0) par 10
D'où : (10;-10) est une solution particulière de (E)

Soit (x;y) une solution de (E) :
On a : $\begin{cases} 3x+2y=10 \\ 3\times(10)+2\times(-10)=10 \end{cases}$ d'où : 3x + 2y = 3×10 + 2×(-10)

3(x – 10) = 2(-y – 10) (*)

3 | 2(-y – 10) avec PGCD(3;2) = 1
D'après le théorème de Gauss, 3 | -y – 10
C'est-à-dire : Il existe $k \in \mathbb{Z}$, -y – 10 = 3k

Il existe $k \in \mathbb{Z}$, $y = -3k - 10$

De même, $2 \mid 3(x - 10)$
avec PGCD(3;2) = 1 d'où ; d'après le théorème de Gauss, $2 \mid x - 10$
C'est-à-dire : Il existe $k' \in \mathbb{Z}$, $x - 10 = 2k'$
Il existe $k' \in \mathbb{Z}$, $x = 2k' + 10$

Réciproquement :

On remplace x et y par leurs expressions dans l'égalité (*) :
D'où : $3 \times 2k' = 2 \times 3k$
Donc : $k' = k$
L'ensemble des solutions de l'équation (E) est donc :

S = {(2k + 10 ; -3k – 10), avec $k \in \mathbb{Z}$ }

IV) Petit théorème de Fermat :

Pierre de Fermat (1601-1665) : Magistrat toulousain.
(Voir : le Grand Théorème de Fermat (montré définitivement en 1994 par Sir Andrew Wiles))

1) Enoncé du petit théorème de Fermat :

Soit $a \in \mathbb{Z}$ et p, un nombre premier tel que $p \nmid a$
Alors : $a^{p-1} \equiv 1$ [p] (autrement dit : $p \mid a^{p-1} - 1$)

Démonstration : En exercice

2) Corollaire :

Soit $a \in \mathbb{Z}$ et p, un nombre premier.
Alors : $a^p \equiv a$ [p] (Autrement dit : $p \mid a^p - 1$)

Démonstration : En exercice

Applications : en cryptographie (voir les exercices)