P. G. C. D. – GAUSS & BÉZOUT

I) Diviseurs communs de deux entiers

1) Définitions

- **D1** : Soit a et b deux entiers. Tout entier d divisant à la fois a et b est un <u>*diviseur commun*</u> de a et de b.
- **D2** : On note $D(a\ ;\ b)$ l'ensemble des diviseurs communs **<u>positifs</u>** de a et de b. Par exemple :

$$D(24\ ;\ 30) = \{1\ ;\ 2\ ;\ 3\ ;\ 6\}$$

2) Propriétés *(entiers non nuls)*

- **P1** : $D(a\ ;\ 0) = D(a)$
  (ensemble des diviseurs positifs de a.)
- **P2** : $D(a\ ;\ 1) = \{\ 1\ \}$ **P3** : $D(a\ ;\ b) = D\left(|a|\ ;\ |b|\right)$
- **P4** : Si a est un multiple de b, alors $D(a\ ;\ b) = D(b)$.
- **P5** : Si $a \geq b$ et a non multiple de b, alors $D(a\ ;\ b) = D(b\ ;\ r)$ où r est le reste (qui est non nul) de la division euclidienne de a par b.

3) T1 : Algorithme d'Euclide (grec, III^{e} siècle av. J.-C.)
Soit a et b entiers <u>strictement positifs</u>**,** alors il existe un unique entier positif δ tel que $D(a\ ;\ b) = D(\delta)$

- **Exemple** avec $a = 264$ et $b = 180$.
  $264 = 180 \times 1 + 84$ donc $D(264\ ;\ 180) = D(180\ ;\ 84)$
  $180 = 84 \times 2 + 12$ donc $D(180\ ;\ 84) = D(84\ ;\ 12)$
  $84 = 12 \times 7 + 0$ donc $D(84\ ;\ 12) = D(12)$.
  On a enfin : $\delta = 12$.
  Dans le cas général, on écrit :
  $a = b \times q_1 + r_1$ et $0 \leq r_1 < b$; si r_1 est non nul, on écrit $b = r_1 \times q_2 + r_2$ et $0 \leq r_2 < r_1$…

  On peut présenter ces calculs sous la forme suivante :

264	180
84	1

180	84
12	2

84	12
0	7

  Ou directement sous la forme suivante :

a	b	r_1	...	r_{n-2}	r_{n-1}
b	r_1	r_2	...	r_{n-1}	r_n
q_1	q_2	q_3	...	q_n	q_{n+1}
r_1	r_2	r_3	...	r_n	0

264	180	84
180	84	12
1	2	7
84	12	0

<u>δ est donc le dernier reste non nul dans les divisions euclidiennes successives</u>

E1 : Appliquer l'algorithme à :

$a = 2916$ et $b = 792$

$a = 2029$ et $b = 393$

E2 : Déterminer, grâce à l'algorithme d'Euclide, le PGCD des deux entiers : 18 996 et 17 724.

II) Plus Grand Commun Diviseur (PGCD)

1) D3 : L'entier δ vérifiant $D(a\ ;\ b) = D(\delta)$ est le <u>*plus grand commun diviseur*</u> de a et de b. Il est noté PGCD(a ; b).

2) Propriétés *(entiers non nuls)*

- **P6** : Le PGCD δ est donc le plus grand élément de $D(a\ ;\ b)$, et il est aussi un multiple de tous ses autres éléments. Autrement dit, tout diviseur commun de deux entiers divise leur PGCD.

- **Exemple** : On a vu que $D(24\ ;\ 30) = \{1\ ;\ 2\ ;\ 3\ ;\ 6\}$. Ainsi, le PGCD de 24 et de 30 est 6, qui est bien le plus grand et aussi un multiple des quatre diviseurs positifs communs de 24 et 30.
- **P7** : $\text{PGCD}(a\ ;\ b) = \text{PGCD}(b\ ;\ a) = \text{PGCD}\left(|a|\ ;\ |b|\right)$
- **P8** : $\text{PGCD}(a\ ;\ a) = \text{PGCD}(a\ ;\ 0) = |a|$
- **P9** : $\text{PGCD}(a\ ;\ 1) = 1$
- **P10** : $a \in D(b)$ si et seulement si $\text{PGCD}(a\ ;\ b) = a$
- **P11** : $\text{PGCD}(ka\ ;\ kb) = |k| \times \text{PGCD}(a\ ;\ b)$

E3 : Déterminer le PGCD de 729 et 198, ainsi que de 5103 et 1386.

- **P12** : Soit l'écriture en produit de facteurs premiers de a et de b : $a = \prod_{i \in N^*} p_i^{\alpha_i}$ et $b = \prod_{i \in N^*} p_i^{\beta_i}$.
  Alors $PGCD(a\ ;\ b) = \prod_{i \in N^*} p_i^{\delta_i}$, où, pour tout entier i,
  δ_i est <u>le plus petit des deux entiers</u> α_i et β_i.

E4 : Décomposer en produit de facteurs premiers les deux nombres $a = 2916$ et $b = 792$ et retrouver ainsi son PGCD.

2916		792		Donc :
				2916 =
				et
				792 =
				ainsi le PGCD
				de a et b =
				c'est-à-dire :

E5 : Même exercice avec les nombres
a = **51 205** et b = **97 405**.

III) Nombres premiers entre eux

1) Définition

- **D4** : Deux nombres entiers strictement positifs sont dits *premiers entre eux* lorsque leur PGCD vaut 1.
- Ne pas confondre les expressions « *premier* » (qui concerne un nombre entier) et « *premiers entre eux* » (qui concerne au moins deux nombres entiers). Par exemple : $6 = 2 \times 3$ et $35 = 5 \times 7$ sont premiers entre eux, et pourtant aucun des deux nombres 6 et 35 n'est premier. Rappelons cependant qu'un nombre est premier si et seulement s'il est *premier avec* tout nombre qui lui est inférieur.
- **Rappel** : une fraction est dite *irréductible* (c'est-à-dire : on ne peut pas la *réduire*) si et seulement si ses numérateur et dénominateur sont premiers entre eux.

E6 : Montrer que deux entiers consécutifs sont toujours premiers entre eux.

E7 : Montrer que, pour tous entiers a et b, $ab + 1$ et $ab + a + 1$ sont toujours premiers en eux.

E8 : Est-il vrai que :
a) Si a et b sont premiers entre eux, alors a^2 et b^2 aussi ?
b) Si a et b sont premiers entre eux, alors $a + b$ et $a \times b$ aussi ?

2) Propriétés *(entiers non nuls)*

- **T2** : Soit a et b deux entiers strictement positifs et soit $d = \text{PGCD}(a ; b)$. Alors on peut écrire : $a = d \times a'$ et $b = d \times b'$ avec $\text{PGCD}(a' ; b') = 1$.

Cette propriété permettra de se ramener de façon fort utile dans certains problèmes à des nombres premiers entre eux

- **P13** : Le PGCD de plus de deux nombres peut se calculer de façon récurrente par exemple par :
Si a, b et c sont trois entiers non nuls,
$\text{PGCD}(a ; b ; c) = \text{PGCD}(\text{PGCD}(a ; b) ; c)$
- **P14** : Soit p un nombre premier. Soit a un entier. Si p divise a, alors leur PGCD vaut p, sinon il vaut 1. Deux nombres premiers distincts sont donc premiers entre eux.
- **P15** : Si $\text{PGCD}(a ; c) = 1$, alors
$\text{PGCD}(a ; b) = \text{PGCD}(a ; bc)$.
- **P16** : Si $\text{PGCD}(a ; bc) = 1$, alors
$\text{PGCD}(a ; b) = 1$ et $\text{PGCD}(a ; c) = 1$.
- **P17** : Si a et b sont premiers entre eux, alors a^n et b^n le sont aussi (avec $n \in \mathbf{N}^*$)

E9 : Déterminer les entiers n compris entre 400 et 1000 vérifiant $\text{PGCD}(n ; 5880) = 84$.

E10 : a) Calculer a et b dans $\mathbf{N}^2$ tels que :

$$\begin{cases} a + b = 360 \\ \text{PGCD}(a ; b) = 18 \end{cases}$$

b) Calculer a et b dans $\mathbf{Z}^2$ tels que : $\begin{cases} a \times b = 2700 \\ \text{PGCD}(a ; b) = 6 \end{cases}$

c) Déterminer les entiers naturels a et b vérifiant :

$$\begin{cases} a^2 \times b = 2304 \\ PGCD(a ; b) = 4 \end{cases}$$

d) Déterminer les entiers naturels a et b, dont le PGCD est 9 et tels que $4a^2 - b^2 = 7695$.

IV) Les théorèmes de Bézout et de Gauss

1) T3 : Identité de Bézout

(Étienne Bézout, français, 1730–1783)

Soit a et b deux entiers strictement positifs. a et b sont premiers entre eux si et seulement s'il existe au moins deux entiers u et v tels que $ua + vb = 1$.

- **Remarque** : Le théorème a en fait été énoncé par Claude Gaspard Bachet de Méziriac (1591 – 1639), Bézout en a fait ensuite une généralisation.
- **Preuve et méthode de détermination**, l'*algorithme d'Euclide étendu* :
On peut utiliser l'algorithme d'Euclide et les entiers qui y apparaissent.
$a = b \times q_1 + r_1$, $b = r_1 \times q_2 + r_2$, $r_1 = r_2 \times q_3 + r_3$, ...
et enfin $r_{n-2} = r_{n-1} \times q_n + r_n$ avec $r_n = \text{PGCD}(a ; b)$
On exprime r_n en fonction de r_{n-1} et r_{n-2} (et les termes q_i), puis on « remonte » en remplaçant les r_i par des r_i avec i plus petit (et en gardant toujours des termes q_i), jusqu'à a et b.
- **Exemple** Cherchons u et v tels que : $15u + 22v = 1$
On a $\underline{\mathbf{22}} = \underline{\mathbf{15}} \times 1 + \underline{\mathbf{7}}$ et $\underline{\mathbf{15}} = \underline{\mathbf{7}} \times 2 + \underline{\mathbf{1}}$, donc :
$\underline{\mathbf{1}} = \underline{\mathbf{15}} - \underline{\mathbf{7}} \times 2$ et $\underline{\mathbf{7}} = \underline{\mathbf{22}} - \underline{\mathbf{15}} \times 1$ donc :
$\underline{\mathbf{1}} = \underline{\mathbf{15}} - (\underline{\mathbf{22}} - \underline{\mathbf{15}} \times 1) \times 2$ c'est-à-dire :
$\underline{\mathbf{1}} = 3 \times \underline{\mathbf{15}} - 2 \times \underline{\mathbf{22}}$.
On a donc comme valeurs possibles : $u = 3$ et $v = -2$.
- **Remarque** : Les entiers u et v ne sont uniques, car on pourra vérifier que, pour toute valeur entière de k,
$u = 3 + 22k$ et $v = -2 - 15k$
sont aussi des solutions de $15u + 22v = 1$.

E11 : Déterminer deux entiers u et v tels que :
$2029u + 393v = 1$

E12 : Montrer que pour tout entier k, les nombres $2k + 1$ et $9k + 4$ sont toujours premiers entre eux.

2) T4 : Théorème de Gauss

(Carl Friedrich Gauss, allemand, 1777–1855)

Si a divise bc et si PGCD(a ; b) = 1, alors a divise c.

- En d'autres termes, *« si un nombre divise le produit de deux nombres et est premier avec l'un des facteurs, alors il divise l'autre. »*

3) Propriétés *(entiers non nuls)*

- **P18** : Si un nombre premier divise un produit de deux nombres, alors il divise au moins l'un des deux.
- **P19** : Si un nombre premier divise un produit de deux nombres premiers, alors il est égal à l'un des deux.
- **P20** : Si n est divisible par a et par b, entiers premiers entre eux, alors n est divisible par $a \times b$.

E13 : a) Soit $P(x) = x^2 + ax + b$, avec a et b entiers. Montrer que si r est une racine rationnelle de $P(x)$, alors r est entier.

b) En déduire que, pour tout n entier naturel, $\sqrt{n}$ est soit un entier soit un nombre irrationnel.

E14 : Déterminer les entiers naturels a et b tels que : $a + b = ab$. *(on pourra utiliser le résultat de* **E6***.)*

V) Résolution de l'équation ax + by = c

1) Définition

- **D5** : Une telle équation, dont les coefficients sont des entiers et les inconnues sont recherchées dans l'ensemble des entiers naturels ou relatifs, s'appelle une *équation diophantienne*, du nom du mathématicien grec Diophante d'Alexandrie *(env. 210 apr. J.-C. – env. 290 apr. J.-C.)*

2) Propriétés *(entiers non nuls)*

- **P21** : Soit a et b deux entiers non nuls. On pose d = PGCD(a ; b). Alors il existe alors au moins deux entiers u et v tels que $ua + vb = d$.

E15 : Est-il vrai que :

a) Si un entier naturel n est congru à 1 modulo 7, alors le PGCD de $3n + 4$ et de $4n + 3$ est égal à 7 ?

b) Il n'existe pas d'entiers relatifs x et y tels que : $3x - 24y = 14$?

c) S'il existe un couple de nombres entiers relatifs (u ; v) tel que $ua + vb = 3$, alors PGCD(a, b) = 3 ?

d) Si les entiers x et y sont premiers entre eux, alors les coefficients de l'identité de Bézout correspondante sont aussi premiers entre eux.

- **P22** : **À redémontrer à chaque utilisation**
  Soit a et b deux entiers non nuls. L'équation : $ax + by$ = PGCD(a ; b) dans $\mathbf{Z}^2$ a pour ensemble de solutions $\{(x\,;y) = (x_0 + kb\,;\, y_0 - ka),\, k \in Z\}$,
  où $(x_0\,;y_0)$ est une solution particulière, obtenue par exemple avec l'algorithme d'Euclide étendu.
- **P23** : L'équation $ax + by = c$ n'a de solutions dans $\mathbf{Z}^2$ que si c est un multiple de PGCD(a ; b).

E16 : Déterminer dans $\mathbf{Z}^2$, grâce à l'algorithme d'Euclide, puis le théorème de Gauss, l'ensemble des solutions de l'équation :

a) $39a - 45b = 6$ b) $4a - 6b = 7$

E17 : Alain vend à Béatrice 22 chaises identiques. Béatrice les paie en lui donnant 17 tables identiques, auxquelles elle ajoute 4 Euros. Déterminer le prix d'une chaise et le prix d'une table, sachant que le prix d'une chaise est un nombre entier impair d'euros, inférieur à 100, et que le prix d'une table est un nombre entier d'euros, supérieur à 100.

E18 : Résoudre la congruence : $7x \equiv 2\ [9]$

E19 : Résoudre les systèmes de congruences :

a) $\begin{cases} x \equiv 4[5] \\ x \equiv 8[9] \end{cases}$ b) $\begin{cases} x \equiv -1\,[12] \\ x \equiv 5\,[18] \end{cases}$

E20 : Retrouver une date de naissance

Partie A : Introduction

Soit l'équation (E) : $31m + 12j = N$, où N est un entier donné et m et j deux entiers relatifs.

1) a) Déterminer la solution particulière de l'équation $31m + 12j = 1$ donnée par l'Algorithme d'Euclide.

b) Justifier que (7 ; –18) est aussi une solution particulière de $31m + 12j = 1$.

c) En déduire une solution particulière de l'équation $31m + 12j = N$.

2) Résoudre : (E) : $31m + 12j = N$.

3) En déduire que si $(m_0\,;\, j_0)$ est solution de (E), alors $m_0 \equiv 7N\,[12]$ et $j_0 \equiv 13N\,[31]$.

Partie B : Application

Monsieur A affirme à Madame B :

« *Multipliez votre jour de naissance par 12,*
votre mois de naissance par 31,
additionnez les deux nombres trouvés
et donnez-moi le résultat N, je pourrai
retrouver votre jour et votre mois de naissance ».

On note m_0 le mois de naissance de Mme B et j_0 son jour de naissance. Le problème est donc de trouver $(m_0\,;\, j_0)$ solution de (E) telle que m_0 soit un entier compris entre 1 et 12 et j_0 soit un entier compris entre 1 et 31.

1) Déduire ce qui précède une méthode pour retrouver le mois de naissance m_0 et le jour de naissance j_0.

2) Quelle réponse donner si $m_0 \equiv 0\,[12]$?

Et si $j_0 \equiv 0\,[31]$?

3) Mme B donne N = 242, quels sont ses jour et mois de naissance ?