I. P G C D de deux entiers :

Définition :

- Soit a et b deux entiers naturels non nuls.

Un entier naturel qui divise a et qui divise b est appelé **diviseur commun** à a et b.
L'ensemble des diviseurs communs à a et à b possède un plus grand élément que l'on appelle **le plus grand commun diviseur** de a et b,
On le note PGCD(a ; b) ou $a \wedge b$.

- $a \wedge b \mid a$; $a \wedge b \mid b$; si $k \in D(a, b)$ alors $k \mid a \wedge b$.

Exemples :

- Dans $\mathbb{N}$ l'ensemble des diviseurs de 15 est {1 ; 3 ; 5 ; 15} et l'ensemble des diviseurs de 12 est {1 ; 2 ; 3 ; 4 ; 6 ; 12}

L'ensemble des diviseurs communs à 12 et à 15 est donc D(12 ; 15) = {1 ; 3} . On a alors PGCD(15 ; 12) = 3

- En écrivant l'ensemble des diviseurs de 159390 et l'ensemble des diviseurs de 49005, on peut obtenir PGCD(159390 ; 49005) = 495 ...

Propriétés :

Soit a et b deux entiers naturels non nuls.

- PGCD(a ; b) $\leq$ a
- PGCD(a ; b) $\leq b$
- PGCD(a ; b) = PGCD(b ; a)
- Si b divise a, on a PGCD(a ; b) = b
- PGCD (a ; 1) = 1
- PGCD (a ; a) = a

Propriété – Lemme d'Euclide

Soit a et b deux entiers naturels non nuls.
Soit q et r le quotient et le reste de la division euclidienne de a par b.

- Si $r = 0$, PGCD(a ; b) = b
- Si $r \neq 0$, PGCD(a ; b) = PGCD(b ; r)

Algorithme d'Euclide :

Soit a et b deux entiers naturels non nuls.
Pour calculer PGCD(a ; b)

- On divise a par b, le reste est r_1
- si $r_1 \neq 0$, on divise b par r_1 ; le reste est r_2
- si $r_2 \neq 0$, on divise r_1 par r_2; le reste est r_3 …………

Il existe un entier n_0 tel que $r_{n_0} \neq 0$ et pour tout $n > n_0$, $r_n = 0$

On a PGCD(a ; b) = r_{n_0}

Exemples :

Pour déterminer le PGCD de 410258 et de 126 écrivons les divisions euclidiennes successives :

$410258 = 126 \times 3256 + 2$

$126 = 2 \times 63 + 0$

Donc PGCD(410258 ; 126) = 2

Pour déterminer le PGCD de 15648 et de 657 écrivons les divisions euclidiennes successives :

$15648 = 657 \times 23 + 537$

$657 = 537 \times 1 + 120$

$537 = 120 \times 4 + 57$

$120 = 57 \times 2 + 6$

$57 = 6 \times 9 + 3$

$6 = 3 \times 2 + 0$

Donc PGCD(15648 ; 657) = 3

Extension de la notion sur Z :

Théorème et définition :

Si a et b sont deux entiers non nuls alors il existe un unique entier naturel d qui vérifie les deux conditions suivantes :

- $d \mid a$ et $d \mid b$
- Si un entier $k \mid a$ et $k \mid b$ alors $k \mid d$.

L'entier d ainsi défini est noté $a \wedge b$ et appelé plus grand commun diviseur de a et b.

Conséquences :

- Pour tous entiers a et b non nuls, $\boldsymbol{a \wedge b > 0}$ et $\boldsymbol{a \wedge b = |a| \wedge |b|}$.
- Si $b \mid a$ alors $a \wedge b = |b|$.
- Si b ne divise pas a et si $a = bq + r$; $0 \leq r < |b|$ alors $a \wedge b = b \wedge r$.
- $a \wedge b = b \wedge a$.
- $\forall k \in \mathbb{Z}^*$, $ka \wedge kb = |k|(a \wedge b)$.
- Si $k \mid a$ et $k \mid b$ alors $\left(\frac{a}{k} \wedge \frac{b}{k}\right) = \frac{a \wedge b}{|k|}$.
- $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Activité 7 page 64 :

1) $2921 = 162 \times 18 + 5 \Rightarrow -2921 = -163 \times 18 + 13 \Rightarrow q = -163$ et $r = 13$.

2) a et $b \in \mathbb{Z}$ tels que : $\begin{cases} a - b = -2921 \\ a \wedge b = 18 \end{cases}$

$a \wedge b = 18 \Rightarrow 18|a$ et $18|b \Rightarrow 18|b - a \Rightarrow 18|2921$ absurde car $2921 = 162 \times 18 + 5$.

II. Entiers premiers entre eux :

Définition :

Soit a et b deux entiers relatifs non nuls.
On dit que a et b sont **premiers entre eux** si leur PGCD est égal à 1.

Activité 1 page 164.

$n \in \mathbb{Z}$ et $d \in \mathbb{N}^*$.

1) Si $d \mid n + 1$ et $d \mid n + 9$ alors $d \mid (n + 9) - (n + 1)$; c à d $d \mid 8$.

2) Si n est pair alors $n \equiv 0 \pmod 2 \Rightarrow n + 1 \equiv 1 \pmod 2$ et $n + 9 \equiv 1 \pmod 2 \Rightarrow n + 1$ et $n + 9$ sont impairs.

Soit $d = (n + 1) \wedge (n + 9) \Rightarrow d \mid n + 1$ et $d \mid n + 9 \Rightarrow d \mid 8 \Rightarrow d \in \{1, 2, 4, 8\}$
Puisque 2, 4 et 8 ne peuvent pas être des diviseurs de $n + 1$ et $n + 9$ qui sont impairs $\Rightarrow d = 1$.

Théorème :

Soit a et b deux entiers relatifs non nuls. Alors il existe un unique couple d'entiers (a', b') tel que :

$a = (a \wedge b) \times a'$; $b = (a \wedge b) \times b'$ et $a' \wedge b' = 1$.

Demonstration:

Posons $d = a \wedge b \Rightarrow \frac{a}{d} = a' \in \mathbb{Z}$ et $\frac{b}{d} = b' \in \mathbb{Z}$ avec $\left(\frac{a}{d} \wedge \frac{b}{d}\right) = \frac{a \wedge b}{|d|} = \frac{d}{d} = 1 \Rightarrow a' \wedge b' = 1$.

Définition :

Lorsque a et b ($b \neq 0$) sont premiers entre eux, on dit que la fraction $\frac{a}{b}$ est irréductible.

D'après ce qui précède, toute fraction $\frac{a}{b}$ est égale à une fraction irréductible $\frac{a'}{b'}$

Activité 3 page 165.

$n \in \mathbb{Z}$, $a = n - 2$ et $b = 3n + 1 \Rightarrow a \wedge b$?

soit $d = a \wedge b \Rightarrow d \mid n - 2$ et $d \mid 3n + 1 \Rightarrow d \mid (3n + 1) - 3(n - 2) \Rightarrow d \mid 7 \Rightarrow d = 1$ ou $d = 7$.

- Si $d = 7 \Rightarrow n - 2 \equiv 0 \pmod 7 \Rightarrow n \equiv 2 \pmod 7 \Rightarrow 3n + 1 \equiv 0 \pmod 7$
  Ainsi $n \equiv 2 \pmod 7 \Leftrightarrow a \wedge b = 7$.
- $a \wedge b = 1 \Leftrightarrow$ n n'est pas congrus à 2 modulo 7.

Activité 4 page 165.

Soit a et b deux entiers relatifs non nuls tels que : $a \wedge b = 1$.

1) Soit $c \in \mathbb{Z}^*$. $ac \wedge bc = |c|(a \wedge b) = |c|$.
2) Si $a \mid bc$ alors $a \mid ac$ et $a \mid bc \Rightarrow a \mid ac \wedge bc \Rightarrow a \mid |c| \Rightarrow a \mid c$.

Lemme de Gauss :

Soit a, b et c trois entiers non nuls. Si $a \wedge b = 1$ et $a \mid bc$ alors $a \mid c$.

Activité 5 page 165.

$(E) : 43x + 71y = 0$.

1) (a, b) est solution de $(E) \Leftrightarrow 43a + 71b = 0 \Leftrightarrow 43(-a) = 71b \Rightarrow 43 \mid 71b$ or $43 \wedge 71 = 1 \Rightarrow 43 \mid b$.
   De plus on a : $71(-b) = 43a \Rightarrow 71 \mid 43a$ or $43 \wedge 71 = 1 \Rightarrow 71 \mid a$.
2) (a, b) est solution de $(E) \Rightarrow a = 71k$, $k \in \mathbb{Z}$ et $43 \times 71k + 71b = 0 \Rightarrow b = -43k \Rightarrow (a, b) = (71k, -43k)$.
   Si $(a, b) = (71k, -43k)$ alors $43a + 71b = 0 \Rightarrow (a, b)$ est solution de (E).
   $S_{\mathbb{Z}\times\mathbb{Z}} = \{(71k, -43k) \ ; k \in \mathbb{Z}\}$.

Activité 7 page 167.

1) $187 \mid n \Rightarrow n = 187 \times q = 11 \times 17 \times q \Rightarrow 11 \mid n$ et $17 \mid n \Rightarrow n \equiv 0[11]$ et $n \equiv 0\ [17]$.
   Inversement si $11 \mid n$ et $17 \mid n \Rightarrow n = 11 \times q$ et $17 \mid 11 \times q \Rightarrow 17 \mid q$ car $17 \wedge 11 = 1 \Rightarrow q = 17 \times q'$

$\Rightarrow$ n = 11 × 17 × q' = 187 × q'.

2) Si 2 | n et 28 | n $\Rightarrow$ 56 | n : <u>non</u> car Si 2 | 84 et 28 | 84 mais 56 ne divise pas 84.

3) Soit a et b deux entiers naturels non nuls tels que : $a \wedge b = 1$

Si a | n et Si b | $n \Rightarrow$ n = a × q et b | n

$b \mid a \times q$ et $a \wedge b = 1 \Rightarrow b \mid q \Rightarrow q = b \times q' \Rightarrow$ n = $a \times b \times q' \Rightarrow a \times b \mid$ n.

Théorème :

Soit a et b deux entiers naturels non nuls et n un entier.

Si $\begin{cases} a \wedge b = 1 \\ n \equiv 0[a] \Rightarrow n \equiv 0[ab] \\ n \equiv 0[b] \end{cases}$

Activité 8 page 167.

$129286 \equiv 1[13]$

$129286 \equiv 1[17]$

$13 \wedge 17 = 1 \Rightarrow 129286 \equiv 1[221]$.

III. P P C M de deux entiers

Théorème et définition :

Pour tous entiers a et b non nuls, il existe un unique entier m > 0 qui vérifie les deux conditions suivantes :

- m est un multiple de a et b.
- Tout multiple commun de a et b est un multiple de m.

L'entier m ainsi défini le plus petit commun multiple de a et b et est noté $a \vee b$.

Conséquences :

- Pour tous entiers a et b non nuls, $\boldsymbol{a \vee b > 0}$ **et** $\boldsymbol{a \vee b = |a| \vee |b|}$.
- Pour tous entiers a et b non nuls, $\boldsymbol{(a \vee b) \times (a \wedge b) = |ab|}$.
- Si b | a alors $a \vee b = |a|$.
- $\forall$ k $\in \mathbb{Z}^*$, $ka \vee kb = |k|(a \vee b)$.
- Si k | a et k | b alors $\left(\dfrac{a}{k} \vee \dfrac{b}{k}\right) = \dfrac{a \vee b}{|k|}$.
- $a \vee b = b \vee a$.
- $a \vee (b \vee c) = (a \vee b) \vee c$.

Activité 2 page 168.

Activité 3 page 168.

$(S) : \begin{cases} ab = -1176 \\ a \vee b = 84 \end{cases}$

Notons par d = $a \wedge b$ et m = $a \vee b \Rightarrow$ m × d = | ab | = 1176 $\Rightarrow$ d = 14

$a = 14a'$; $b = 14b'$ et $a' \wedge b' = 1$

$ab = -1176 \Rightarrow a'b' = -6 \Rightarrow (a', b') = \{(1, -6) ; (-6, 1) ; (-1, 6) ; (6, -1) ; (2, -3) ; (-3, 2) ; (-2, 3) ; (3, -2)\}$

$\Rightarrow$ *(a, b)* = {(14, -84) ; (-84, 14) ; (-14, 84) ; (84, -14) ; (28, -42) ; (-42, 28) ; (-28, 42) ; (42, - 28) }.

$(S') : \begin{cases} ab = 168 \\ a \vee b = 24 \end{cases} \Rightarrow a \wedge b = 7 \Rightarrow a = 7a' \,;\, b = 7b'$ et $a' \wedge b' = 1 \Rightarrow a'b' = \dfrac{168}{49} \notin \mathbb{Z}$ impossible

$S_{\mathbb{Z}\times\mathbb{Z}} = \varnothing$.

Activité 5 page 168.

1) a) $a \equiv 0[8]$ et $a \equiv 0[12] \Rightarrow a \in (8\mathbb{Z}) \cap (12\mathbb{Z}) \Rightarrow a \in (8 \vee 12)\mathbb{Z} \Rightarrow a \in 24\mathbb{Z} \Rightarrow a \equiv 0[24]$.
   b) Inversement : si $a \equiv 0[24]$ alors $a = 24k = 8 \times (3k) = 12 \times (2k) \Rightarrow a \in (8\mathbb{Z}) \cap (12\mathbb{Z})$

2) $a \equiv 1[8]$; $a \equiv 1[12]$ et $a \leq 225 \Rightarrow a - 1 \equiv 0[8]$; $a - 1 \equiv 0[12]$ et $a \leq 225 \Rightarrow a - 1 \equiv 0[24]$ et $a - 1 \leq 224$.

   $\Rightarrow a \in \{$ -215, -191, - 167, -143, -119, -95, -71, -47, -28, 1, 25, 49, 73, 97, 121, 145, 169, 193, 217$\}$.

IV. Inverses modulo b :

Activité 1 page 168.

1) a) u $\in \mathbb{Z}$

u ≡ ….[9]	0	1	2	3	4	5	6	7	8
6u ≡ …..[9]	0	6	3	0	6	3	0	6	3

   b) Il n'existe aucun un entier u tel que 6u ≡ 1[9]

2) - 34 = 7 × (-5) + 1 ⇒ -34 ≡ 1[7] ⇒ u = -1 est une solution.

Théorème :

Soit a et b deux entiers naturels non nuls tels que $b \geq 2$ et $a \wedge b = 1$.

Il existe un unique entier non nul u appartenant à $\{0, 1, \ldots\ldots\ldots, b - 1\}$ tel que au ≡ 1[b].

On dit que u est un inverse de a modulo b.

Exercice :

On considère l'ensemble $A_7 = \{1, 2, 3, 4, 5, 6\}$.

a) Pour tout élément a de A_7, écrire dans le tableau suivant (sans justifier) l'unique élément y de A_7 tel que ay ≡ 1[7].

a	1	2	3	4	5	6
y						

b) Pour x entier relatif, démontrer que l'équation $3x \equiv 5[7]$ équivaut à $x \equiv 4\{7]$.

c) Si a est un élément de A_7, montrer que les seuls entiers relatifs x solutions de l'équation $ax \equiv 0[7]$ sont les multiples de 7.

V. Identité de Bézout :

Activité 1 page 170.

1) a) 25u ≡ 1[13]
   25 × 12 = 300 = 23 × 13 + 1 ⇒ 12 est un inverse modulo 13 de 25.

b) $25 \times 12 + 13 \times (-23) = 1 \Rightarrow (u, v) = (12, -23)$.

2) $27u + 10v = 1$; $(u, v) = (3, -8)$.

3) $9 \times (-3) + 14 \times 2 = 1$; $9 \times 1 + 8 \times (-1) = 1$.

Théorème de Bézout :

Soit a et b deux entiers relatifs non nuls.

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

Preuve :

- Supposons qu'il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Soit D le PGCD de a et b, alors D divise a et D divise b, donc D divise $au + bv$. Donc D divise 1. Donc D = 1.
On en déduit alors que a et b sont premiers entre eux.

- Supposons que a et b sont premiers entre eux.

Considérons l'ensemble E des entiers naturels non nuls de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$.
E n'est pas vide (E contient a ou $-a$, E contient b ou $-b$, E contient $2a + 3b$ ou $-2a - 3b$ ...), donc E a un plus petit élément m.
On peut écrire $m = au_1 + bv_1$ avec $u_1 \in \mathbb{Z}$ et $v_1 \in \mathbb{Z}$.
Écrivons la division euclidienne de a par m : $a = mq + r$ avec $r \in \mathbb{N}$ et $0 \leq r < m$.
On a alors : $a = (au_1 + bv_1)\, q + r \Rightarrow r = a - (au_1 + bv_1)q \Rightarrow r = a\,(1 - u_1\, q) + b\,(-v_1\, q)$
Donc r est un entier naturel de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ et d'autre part $r < m$.
Comme m est le plus petit élément de E, on en déduit que $r = 0$, c'est-à-dire que a est divisible par m.

De même on démontrerait que b est divisible par m.
Donc m est un diviseur commun à a et b.
Comme a et b sont premiers entre eux, on en déduit que $m = 1$.
On a donc $1 = au_1 + bv_1$ avec $u_1 \in \mathbb{Z}$ et $v_1 \in \mathbb{Z}$.

Corollaire :

Soit a et b deux entiers relatifs non nuls.
Si D = PGCD(a ; b) , alors il existe deux entiers relatifs u et v tels que $au + bv = D$.

VI. Exemples d'équations de la forme $ax + by = c$; a, b et c entiers

Activité 1 page 171.

a, b et $c \in \mathbb{Z}$; $d = a \wedge b$;

1) d ne divise pas c
Supposons qu'il existe deux entiers x et y tels que $ax + by = c$
$d \mid a$ et $d \mid b \Rightarrow d \mid ax + by \Rightarrow d \mid c$ absurde (E) n'a pas de solutions.
2) $d \mid c \Rightarrow c = dk$, or $d = a \wedge b \Rightarrow$ il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que : $au + bv = d$
$\Rightarrow c = (au + bv)k = a(uk) + b(vk) \Rightarrow (uk, vk)$ est une solution de (E).

Théorème :

Soit a, b et c trois entiers et $d = a \wedge b$. L'équation $ax + by = c$ admet des solutions dans $\mathbb{Z} \times \mathbb{Z}$, si et seulement si, d divise c.

Activité 2 page 171.

(E) : $2x + 3y = 1$.

1) (-1, 1) est une solution de (E).

2) a) Soit (x, y) une solution de (E) $\Rightarrow 2x + 3y = 1$, or $2 \times (-1) + 3 \times 1 = 1 \Rightarrow 2(x + 1) + 3(y - 1) = 0$

$\Rightarrow 2(x + 1) = -3(y - 1) \Rightarrow 2 \mid 3(y - 1)$ et $3 \mid 2(x + 1)$, or 2 et 3 sont premiers entre eux $\Rightarrow 2 \mid y - 1$ et $3 \mid x + 1$

$\Rightarrow y - 1 = 2k \Rightarrow y = 1 + 2k$, $2x + 3y = 1 \Rightarrow x = -1 - 3k$

$S_{\mathbb{Z}\times\mathbb{Z}} = \{(-1 - 3k, 1 + 2k) \ ; \ k \in \mathbb{Z}\}$

3) $2x + 3y = 5$.

(-5, 5) est une solution particulière…..