Aptitudes à développer :

*Reconnaître que deux entiers sont premiers entre eux,
en utilisant la relation de Bézout.
*Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ des équations du type : ax + by = c
avec a, b et c entiers relatifs.

Plan du chapitre :

I - Entiers premiers entre eux

II - PGCD de deux entiers

III- PPCM de deux entiers

IV- Exemples d'équations de la forme ax + by = c ; a, b et c entiers

L-P-Bourguiba deTunis		Prof :Ben jedidia chokri
Chapitre 8	Identité de Bézout	Classe :4 Math

I- PGCD de deux entiers

0n rappelle que si a et b sont deux entiers naturels non nuls alors leur plus grand commun diviseur est l'entier naturel $a \wedge b$ tel que $a \wedge b$ divise a et b et tout diviseur commun à a et b divise $a \wedge b$.

Le plus grand diviseur commun de deux entiers naturels a et b est le dernier reste non nul dans la succession des divisions euclidiennes de l'algorithme d'Euclide de a et b.

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 :

1. d divise a et d divise b,
2. Si un entier k divise a et b alors il divise d.

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

Preuve :

D_a : Diviseurs de a

D_b : Diviseurs de b

$D_a \cap D_b$: Ensemble non vide $(1 \in D_a \cap D_b)$

$d \in D_a \cap D_b$

$a \geq b \qquad |d| \leq |a|$

$D_a \cap D_b \neq \phi$

$D_a \cap D_b \subset \mathbb{Z}$

$D_a \cap D_b$: majoré

$D_a \cap D_b$ admet un plus grand élément $a \wedge b$

Exemple :

$$\begin{cases} a = 465 \\ b = 225 \end{cases}$$

$$\begin{array}{r||l} 465 & 3 \\ 155 & 5 \\ 31 & 31 \\ 1 & \end{array} \qquad \begin{array}{r||l} 225 & 3 \\ 75 & 3 \\ 25 & 5 \\ 5 & 5 \\ 1 & 1 \end{array}$$

$465 = 3 \times 5 \times 31 \qquad 225 = 3^2 \times 5^2$

$D_{465} = \{1,3,5,15,31,93,115,465,-1,-3,-5,-15,-31,-93,-155,-465\}$

$D_{225} = \{1,3,9,5,25,15,45,75,225,-1,-3,-9,-5,-25,-15,-45,-75,-225\}$

$D_{465} \cap D_{225} = \{1,3,5,15,-1,-3,-5,-15\}$

15 est le plus grand élément de $D_{465} \cap D_{225}$

$\Rightarrow 465 \wedge 225 = 15$

$$\begin{cases} a = 196 \\ b = 116 \end{cases} \quad \begin{matrix} 196 = 2^2 \times 7^2 \\ 116 = 2^2 \times 29 \end{matrix} \Rightarrow a \wedge b = 196 \wedge 116 = 4$$

$$\begin{cases} a = 144 \\ b = 388 \end{cases} \quad \begin{matrix} 388 = 2^2 \times 97 \\ 144 = 2^4 \times 3^2 \end{matrix} \Rightarrow 388 \wedge 144 = 4$$

Algorithme d'euclide :

$\begin{cases} a = 19625 \\ b = 1155 \end{cases}$ la calculatrice donne 16 ⌈229 ⌈ 231

$19625 = 1155 \times 16 + 1145$

$1155 = 1145 \times 1 + 10$

$10 = 5 \times 2 + 0$

le dernier reste non nul dans l'algorithme d'Euclide est 5

$\Rightarrow 19625 \wedge 1155 = 5$

EXPLCATION :

$a = b \times q_1 + r_1 \qquad 0 \le r_1 < b \qquad r_1 \ne 0$

$a = r_1 \times q_2 + r_2 \qquad 0 \le r_2 < r_1 \qquad r_2 \ne 0$

$r_1 = r_2 \times q_3 + r_3 \qquad 0 \le r_3 < r_2$

.

.

.

$r_{n-2} = r_{n-1} \times q_n + r_n$

$r_{n-1} = r_n q_{n+1} + 0$

le processus s'arrête et on a $r_{n-1} = r_n q_{n+1}$

(r_n) une suite d'entiers naturels décroissante $\Rightarrow r_{n+1} = 0$

$a \wedge b = b \wedge r_1 = ... = r_{n-2} \wedge r_{n-1} = r_{n-1} \wedge r_n = r_n$

Propriétés

Soit a et b deux entiers non nuls.

- Si b divise a alors $a \wedge b = |b|$.
- Si b ne divise pas a et si r est le reste modulo b de a alors $a \wedge b = b \wedge r$.
- $a \wedge b = b \wedge a$.
- Pour tout entier non nul k, $ka \wedge kb = |k|(a \wedge b)$.
- $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

II- Entiers premiers entre eux

Définition

Deux entiers non nuls a et b sont dits premiers entre eux, si $a \wedge b = 1$.

Théorème

Soit a et b deux entiers non nuls. Alors il existe un unique couple d'entiers (a',b') tel que $a = (a \wedge b)a', b = (a \wedge b)b'$ et $a' \wedge b' = 1$.

démonstration :

posons $d = a \wedge b$

$$\begin{cases} d \mid a \\ d \mid b \end{cases} \Rightarrow \begin{cases} a = da' \\ b = db' \end{cases}$$

$$\Rightarrow d = a \wedge b = da' \wedge db'$$
$$= d(a' \wedge b')$$
$$\Rightarrow a' \wedge b' = 1$$

(Unicité facile)

Lemme de Gauss

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

Démonstration :

$$\text{on} \begin{cases} a \mid ac \\ a \mid bc \end{cases} \Rightarrow a \mid ac \wedge bc$$
$$\Rightarrow a \| c \mid (a \wedge b)$$
$$\Rightarrow a \| c \mid$$
$$\Rightarrow a \mid c$$

Théorème

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

Si $a \wedge b = 1$, $n \equiv 0$ (mod a) et $n \equiv 0$ (mod b) alors $n \equiv 0$ (mod ab).

$$\begin{matrix} n \equiv 0[a] \\ n \equiv 0[b] \end{matrix} \Rightarrow \begin{cases} a \mid n \\ b \mid n \end{cases} \Rightarrow \begin{cases} n = Ka \\ n = K'b \end{cases}$$
$$\Leftrightarrow Ka = K'b = n$$

$$\begin{cases} a \mid Ka = K'b \\ a \wedge b = 1 \end{cases}$$
$$\Rightarrow a \mid K'(\text{Gauss})$$
$$\Rightarrow K' = qa$$
$$\Rightarrow n = K'b = qab$$
$$\Rightarrow n \equiv 0[ab]$$

généralisation

$$\text{si} \begin{cases} n \equiv x[a] \\ n \equiv x[b] \\ a \wedge b = 1 \end{cases}$$

III- PPCM de deux entiers

Théorème et définition

Pour tout entiers a et b non nuls il existe un unique entier m strictement positif

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 est le plus petit commun multiple de a et b est noté $a \vee b$.

Conséquences

- Pour tous entiers a et b non nuls, $a \vee b = |a| \vee |b|$.
- Pour tous entiers a et b non nuls, $(a \vee b) x (a \wedge b) = |ab|$

Propriétés

Soit a et b deux entiers non nuls.

- Si b divise a alors $a \vee b = |a|$.
- Pour tout entier non nul k, $ka \vee kb = |k|(a \vee b)$.
- $a \vee b = b \vee a$.
- $a \vee (b \vee c) = (a \vee b) \vee c$.

Théorème

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

Alors il existe un unique entier non nul u appartenant à $\{0,1,\ldots,b-1\}$ tel que $au \equiv 1(\text{mod } b)$.

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

Démonstration :

$$\begin{cases} ma \equiv na(\text{mod}\, b) \\ a \wedge b \equiv 1 \end{cases}$$

$ma - na$ est multiple de b

$$\begin{cases} b \mid (m-n)a \\ a \wedge b = 1 \end{cases} \text{Gauss} \Rightarrow b \mid m - n$$

soit i et j deux entiers tq $1 \leq i \leq j \leq b-1$

b ne divise pas $(j-i)$ car $0 < j - i < b$

ainsi $ia \equiv r_i [b]$

$r_i \in \{0,1 \ldots\ldots\ldots, b-1\}$

par suite il existe $u \in \{1, \ldots\ldots\ldots\ldots\ldots, b-1\}$

tq $ua \equiv 1[b]$

$$\begin{cases} ia \equiv r_i [b] \\ ja \equiv r_j [b] \end{cases}$$

$r_i \neq r_j$

si $r_i = r_j \Rightarrow b \mid i - j$ absurde $0 < i - j < b$

$i \neq j$

V- Identité de Bezout

Théorème de Bezout

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

Démonstration :

$a \wedge b = 1$

il existe $w \in \{1, \ldots\ldots\ldots, b-1\}$

tq $aw \equiv 1 (\mathrm{mod}\, b) \Leftrightarrow aw - kb = 1$

$u = w$ et $v = -k$

*supposons qu'on a : $au + bv = 1$ et démontrons que : $a \wedge b = 1$

posons $d = a \wedge b$

$\Rightarrow d \mid a$ et $d \mid b \Rightarrow d \mid au + bv$ (combinaison linéaire)

$\Rightarrow d \mid 1$

Corollaire

Soit a et b deux entiers non nuls et d = $a \wedge b$. Alors il existe deux entiers u et v tels que au + bv = d.

Démonstration :

$d = a \wedge b$

il existe a' et b' tq $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$

d'après Bézout il existe u et v telque : $a'u + b'v = 1$

$\Rightarrow da'u + db'v = d \Rightarrow au + bv = d$

EXEMPLE :

$22826 = 537 \times 42 + 272$

$237 = 272 \times 1 + 265$

$272 = 265 \times 1 + 7$

$265 = 7 \times 37 + 6$

$7 = 6 \times 1 + 1$

$6 = 1 \times 6 + 0$

le dernier reste non nul dans l'algorithme d'Euclide est1 $\Rightarrow \mathrm{PGCD}(a,b) = 1$; $a \wedge b = 1$

$\Rightarrow 22826$ et 537 sont premiers entre eux

METHODE (reculons)

$$\begin{aligned}
1 &= 7 - 6 \times 1 \\
&= 7 - (265 - 7 \times 37) \\
&= (272 - 265) \times 38 - 265 \\
&= 272 \times 38 - 265 \times 39 \\
&= 272 \times 38 - (537 - 272) \times 39 \\
&= 272 \times 77 - 537 \times 39 \\
&= (22826 - 537 \times 42) \times 77 - 537 \times 39 \\
&= 22826 \times 77 - 537 \times 3273
\end{aligned}$$

$$\begin{cases} u = 77 \\ v = -3273 \end{cases}$$

Méthode (tableau) (procédure /algorithme)

r_i	272	265	7	6	1	0
q_i	42	1	1	37	1	6

<table>
<tr><td colspan="2">q_i</td><td>42</td><td>1</td><td>1</td><td>37</td><td>1</td><td>6</td></tr>
<tr><td>0</td><td>1</td><td>$42 \times 1 + 0 = 42$</td><td>$1 \times 42 + 1 = 43$</td><td>$1 \times 43 + 42 = 85$</td><td>3188</td><td>3273</td><td>22826</td></tr>
<tr><td>1</td><td>0</td><td>$42 \times 0 + 1 = 1$</td><td>$1 \times 1 + 0 = 1$</td><td>$1 \times 1 + 1 = 2$</td><td>75</td><td>77</td><td>537</td></tr>
</table>

$5+1 \leftarrow$ indice du dernier reste non nul

$(-1)^6 \times (22826 \times 77 - 537 \times 3273) = 1$

$$\begin{cases} u = 77 \\ v = -3273 \end{cases}$$

IV- Exemples d'équations de la forme ax + by = c ; a, b et c entiers

Théorème

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

Démonstration :

Si d ne divise pas c

$\Rightarrow d$ ne divise pas $ax+by$ (absurde)

si d divise pas c , $a = da'$

$b = db'$ $\quad a' \wedge b' = 1$

$ax+by = c \Leftrightarrow da'x + db'y = c$

d'après Bézout $a \wedge b = 1$, il existe deux entiers u et v tq au+bv=1

$a'x+b'y=c'$ avec $c=c'd$

or $a' \wedge b' = 1$ d'après Bézout

$a'u + b'v = 1$

$a'c'u + b'c'v = c'$

$(c'u),(c'v)$ est une solution de (E_2) et aussi solution de (E_1)

Exercice :

Résoudre dans $\mathbb{Z} \times \mathbb{Z}$

$11x + 8y = 79$

1er méthode :

$11 \wedge 8 = 1 | 79 \Rightarrow (E)$ admet des solutions dans $\mathbb{Z}^2$

$11 = 8 \times 1 + 3$

$8 = 3 \times 2 + 2$

$3 = 2 \times 1 + 1$

$2 = 1 \times 2 + 0$

$1 = 3 - 2$

$= 3 - (8 - 3 \times 2)$

$= 3 - 8 + 3 \times 2$

$= 3x(11 - 8) - 8$

$= 3 \times 11 - 4 \times 8$

$$\begin{cases} u = 3 \\ v = -4 \end{cases}$$

on a alors $3 \times 11 - 4 \times 8 = 1$

$\Leftrightarrow 237 \times 11 - 316 \times 8 = 79$

$$\begin{cases} x_0 = 237 \\ y_0 = -316 \end{cases}$$

(x,y) sol de E $\Leftrightarrow \begin{cases} 11x + 8y = 79 \\ 11x_0 + 8y_0 = 79 \end{cases}$

$\Leftrightarrow 11(x - x_0) + 8(y - y_0) = 0$

$$\Leftrightarrow 11(x-x_0)=-8(y-y_0)$$

or $11\wedge 8=1 \Rightarrow$ d'après gauss $8\mid x-x_0$

$$\Leftrightarrow x-x_0=8k$$

$$\Leftrightarrow x=8k+x_0=8k+237=8k+5$$

$$11\times 8k=-8(y-y_0)$$

$$\Leftrightarrow y-y_0=-11k$$

$S_{\mathbb{Z}^2}=\{(8k+5;-11k+3),k\in\mathbb{Z}\}$ $\Leftrightarrow y=-11k+y_0=-11k-316$

2emme méthode (congruence)

$$\begin{cases}11\wedge 8=1\\ 1\mid 79\end{cases}\Rightarrow 11x+8y=79$$

admet des solution dans $\mathbb{Z}\times\mathbb{Z}$

$11x\equiv 79(\text{mo}8)$

$3x\equiv 79(\text{mod}\,8)$

$3x\equiv 7(\text{mod}\,8)$

$x\equiv[8]$	0	1	2	3	4	5	6	7
$3x\equiv[8]$	0	3	6	1	4	7	2	5

On a $3\times 5\equiv 7(\text{mod}\,8)$

Donc $x_0=5$

$$y_0=\frac{79-11\times 5}{8}=3$$

$S_{\mathbb{Z}\times\mathbb{Z}}=\{(8k+5;-11k+3),k\in\mathbb{Z}\}$

3ème méthode :

r_i		3	2	1	0
q_i		1	2	1	2
q_i		1	2	1	2
0	1	1	3	4	11
1	0	1	2	3	8

On a $(-1)^4\times(11\times 3-8\times 4)=1$