feuille n°1

Chapitre 4 **Les théorèmes fondamentaux : Bezout , Gauss et Fermat**

I] Identité et Théorème de Bezout :

1) Identité de Bezout :

Si a et b sont des entiers relatifs non nuls et d leur PGCD alors il existe deux entiers relatifs u et v tels que $\boxed{au + bv = d}$

Démonstration : Approche :

a	b	reste	Division euclidienne de a par b	Expression des restes en fonction de a et b
a	b	r_1	$a = bq_1 + r_1$	$r_1 = \boxed{a - bq_1}$
b	r_1	r_2	$b = r_1 q_2 + r_2$	$r_2 = b - r_1 q_2$ $= b-(a-bq_1)q_2$ $= \boxed{-aq_2 + (1+bq_1q_2)b}$
r_1	r_2 etc	r_3 etc	$r_1 = r_2 q_3 + r_3$	$r_3 = r_1 - r_2 q_3$ $\boxed{= (a-bq_1) - [b-(a-bq_1)q_2]q_3}$ par substitution

On peut donc exprimer tous les restes en fonction de a et b , en particulier le dernier reste non nul qui est égal au PGCD (a , b) = d et donc il existe 2 entiers u et v tels que d = a u + b v

La démonstration exacte se fait à l'aide d'un raisonnement par récurrence

3) Théorème de Bezout :

a) **Théorème :** **Soient a et b deux entiers relatifs non nuls**

a et b sont premiers entre eux ssi il existe deux entiers relatifs u et v tels que $\boxed{au + bv = 1}$

b) Démonstration : ROC à savoir

*) Si a et b sont premiers entre eux alors PGCD(a,b) = 1 et d'après l'identité de Bezout il existe 2 entiers relatifs $au + bv = PGCD(a,b) = 1$

*) Réciproque : Si au + bv = 1 et si d est un diviseur positif commun de a et de b alors d divise toute combinaison linéaire de a et b par ex $au + bv = 1$ donc d divise 1. Or le seul diviseur positif de 1 est 1 donc $\boxed{d = 1}$. Donc comme tout diviseur commun de a et b divise le PGCD (a,b). On a donc d = 1 divise le PGCD(a,b) et donc $\boxed{PGCD(a,b) = 1}$

c) Remarque : le couple (u, v) n'est **pas unique . u et v** sont appelés **les coefficients de Bezout**

d) Exemple : 1) En utilisant l'algorithme d' Euclide , démontrer que 392 et 33 sont premiers entre eux
2) En déduire deux entiers relatifs u et v tels que 392 u + 33 v = 1

a	b	reste	Division euclidienne de a par b	Reste en fonction de a et b
392	33	$r_1 = 29$	$392 = 11 \times 33 + 29$	$r_1 = a - 11b$
33	29	$r_2 = 4$	$33 = 1 \times 29 + 4$	$r_2 = b - 1r_1$ $= b - (a - 11b)$ $r_2 = -a + 12b$
29	4	$r_3 = 1$	$29 = 7 \times 4 + 1$	$r_3 = r_1 - 7r_2$ $= a - 11b - 7(-a + 12b)$ $r_3 = 8a - 95b$
4	1	$r_4 = 0$	$4 = 4 \times 1 + 0$	—

le dernier reste non nul est $r_3 = 1 = PGCD(a,b)$ donc a = 392 et b = 33 sont premiers entre eux.

et $r_3 = 1 = 8a - 95b$ donc $\boxed{u = 8 \text{ et } v = -95}$ conviennent

$\boxed{1 = ua + vb}$ et $1 = 8 \times 392 - 95 \times 33$, et on a $\boxed{392u + 33v = 1}$

on cherche les points de coordonnées entières sur la droite d'équation $y = \frac{-392}{33}x + \frac{1}{33}$ feuille n°2

Remarque : On peut aussi trouver un couple (u , v) à l'aide de la calculatrice

Par exemple : dans l'ex précédent on doit trouver x et y entiers tels que $\boxed{392\,x + 33\,y = 1}$

u= x et v= y On exprime y en fonction de x : y = $\frac{1-392x}{33}$ Et on introduit cette fonction affine dans f(x) puis dans 2^{nd} fenêtre soit déf tab : deb tbl= 0 et 2^{nd} graph et on cherche le couple (x, y) entiers

pas = 1

On retrouve x = 8 = u et y = - 95 = v ou $x = u = 16$, $y = v = -190$ ou $x = u = -25$, $y = v = 297$

e) Algorithme et Programme pour déterminer les coefficients de Bezout :

Entrées	*a ; b*
Initialisation	*u* prend la valeur 1, *v* prend la valeur 0
	x prend la valeur 0, *y* prend la valeur 1
	c prend la valeur 0, *d* prend la valeur 0
Traitement	Tant que $b > 0$
	q prend la valeur Partie Entière (a / b) ; *r* prend la valeur $a - bq$;
	c prend la valeur *u* ; *d* prend la valeur *v* ;
	u prend la valeur *x* ; *v* prend la valeur *y* ;
	x prend la valeur $c - xq$; *y* prend la valeur $d - yq$;
	a prend la valeur *b* ; *b* prend la valeur *r* ;
	Fin du Tant que
Sortie	Afficher *a*, *u* et *v*

```
PROGRAM:BEZOUT
:Input "A=",A
:Input "B=",B
:1→U
:0→V
:0→X
:1→Y
:While B>0
:int(A/B)→Q
:A-B*Q→R
:U→C
:V→D
:X→U
:Y→V
:C-Q*X→X
:D-Q*Y→Y
:B→A
:R→B
:End
:Disp "PGCD=",A
:Disp "U=",U
:Disp "V=",V
```

II -] Théorème de Gauss :

1) Théorème de Gauss :

Si un entier a <u>divise le produit bc</u> et si <u>a et b sont premiers entre eux</u> alors …a… divise c

Démonstration : **ROC à savoir**

*) Si a est premier avec b alors PGCD(a, b) = 1 et d'après le théorème de Bezout il existe 2 entiers u et v tels que $au + bv = 1$

En multipliant par c cette relation on obtient $acu + bcv = c$

*) Et si a divise bc , comme a divise ac et bc alors a divise toute combinaison linéaire des 2 donc a divise $acu + bcv = c(au + bv) = c \times 1 = c$

donc a divise c

2) Conséquences :

a) Si a et b divisent un entier c alors ……ab divise c ou si a et b premiers entre eux et si $c \equiv 0(a)$ et $c \equiv 0(b)$ alors $c \equiv 0(ab)$

et si a et b premiers entre eux

A SAVOIR

Démonstration : Si a divise c alors ……il existe un entier k tel que $\boxed{c = ka}$

Si b divise c alors ……… b divise $ka = c$

Et si a et b premiers entre eux alors …d'après le th de Gauss b divise k

donc il existe un entier k' tel que $\boxed{k = k'b}$ et donc $\boxed{c = k'ba}$ et ab divise c

b) Si un nombre <u>premier p</u> <u>divise</u> le produit <u>ab</u> alors p <u>divise</u> …a…ou…b..

si p premier et si $ab \equiv 0(p)$ alors $a \equiv 0(p)$ ou $b \equiv 0(p)$

Démonstration : Si p nombre premier divise ab :

distinguons <u>2 cas :</u> *) Si p divise a alors ……p divise a ou b est vérifiée

*) Si p ne divise pas a alors comme p premier , les diviseurs positifs de p sont … 1 et p

Les valeurs possibles du PGCD (a ; p) sont donc ……1 ou p . or comme p ne divise pas a alors PGCD(a, p) ≠ p et donc PGCD(a, p) = 1 donc a et p premiers entre eux et p divise (ab) donc d'après le th de Gauss, p divise b et $\boxed{\text{p divise a ou b}}$

c) Si un nombre <u>premier</u> p <u>divise un produit qc</u> de nombres <u>premiers</u> alors p est égal à ……q ou… a c

si p premier et si $qc \equiv 0(p)$ avec q et c premiers alors $p = q$ ou $p = c$

III -] Equations diophantiennes :

1) Définition : Soient **a et b 2 entiers**

Elles consistent à **chercher** 2 nombres **<u>entiers</u> x** et **y** tels que **ax + by = c** ,avec , pour application immédiate , la recherche d'éventuels points situés sur une droite donnée et dont les deux coordonnées sont des entiers feuille n°3

2) Méthode : Résolution de $ax + by = c$

a) On détermine le PGCD $(a, b) = d$

b) Distinguons 2 cas :

*) 1° cas : **Si d ne divise pas c , alors l'équation n'a pas de solution** entière

*) 2° cas : **si d divise c** alors

*) On commence par chercher une **solution particulière** (x_0, y_0) à cette équation à moins que cette solution soit **évidente** soit **donnée** dans l'énoncé . Pour la trouver, on utilise **l'algorithme d'euclide** ; on peut aussi utiliser la calculatrice .

(Remarquez qu' il y a une infinité de solutions possibles)

*) On a donc le système suivant : $\begin{cases} ax + by = c \\ ax_0 + by_0 = c \end{cases}$ on obtient alors par substitution $ax + by = ax_0 + by_0$

d'où en regroupant les a dans un membre et les b dans l'autre on obtient :

$$a(x - x_0) = b(y_0 - y)$$

*) On utilise **le Théorème de Gauss** pour déterminer la seule forme possible pour les éventuelles solutions

*) Il reste à vérifier la **réciproque** que tout couple de cette forme est bien solution

3) Exemples : a) **Equation du type $ax = by$**

Déterminer les entiers x et y tels que $4x = 3y$

b) **Equation du type $ax + by = c$**

Déterminer les entiers x et y tels que :

1) $5x - 3y = 1$ 2) $12x + 18y = 6$ 3) $4x - 8y = 3$ 4) $2x + 3y = 5$

IV -] Le petit théorème de Fermat

1) Le petit Théorème de Fermat

Soit n un entier . Si p est un nombre premier ne divisant pas n , alors $n^{p-1} \equiv 1 \ (p)$

2) Corollaire :

Si p est un naturel premier et n est un entier naturel alors $n^p \equiv n \ (p)$

3) Exemples : a) **Ex n° 1 :** Montrer que $1^{16} + 2^{16} + 3^{16} + \ldots + 16^{16} + 1$ est divisible par 17

puis que $4^{28} - 1$ est divisible par 29

b) **Ex n°2 :** n désigne un entier naturel supérieur ou égal à 2

On considère l'entier naturel $a = n^5 - n$

A) Démontrer que a est divisible par $n^3 - n$

B) Démontrer que a est divisible par 3 , 2 et 5 donc par 30

Exercice n°1 :

1) $a = 257$ et $b = 45$.

a) Ecrire l'algorithme d'Euclide pour déterminer le PGCD (a , b).

b) En dédire des entiers relatifs u et v tels que $au + bv = $ PGCD (a , b) .

2) Même question avec $a = 383$ et $b = 127$.

Exercice n°2 :

1) Montrer que pour tout entier n , $a = 2n + 1$ et $b = 6n + 4$ sont premiers entre eux .
2) Même question avec $a = n$ et $b = 2n + 1$.
3) Vérifier que $(n^2 + 1)^2 = n(n^3 + 2n) + 1$. Démontrer alors que $n^3 + 2n$ et $n^2 + 1$ sont premiers entre eux .

Exercice n°3 :

a , b et c sont des entiers non nuls . Montrer que l'équation $ax + by = c$ admet des solutions entières ssi c est un multiple de $d = $ PGCD (a , b) .

Exercice n°4 :

a , b et c sont des entiers non nuls . Montrer que si a est premier avec b et si a est premier avec c alors a est premier avec bc .

Exercice n°5 :

1) Déterminer les valeurs de n , entier naturel pour que la fraction suivante soit irréductible :

a) $\dfrac{3n-2}{n+7}$ b) $\dfrac{n^2+6}{n+1}$.

2) Soit n un entier naturel ; on considère la fraction $a = \dfrac{n+7}{n+2}$:

a) Déterminer n tel que a soit un entier naturel .

b) Déterminer n tel que a soit une fraction irréductible .

Exercice n°6 :

a) Déterminer tous les couples (x , y) d'entiers relatifs tels que $7x = 11y$.
b) Vérifier que le couple $(x_0, y_0) = (13, 8)$ est solution de l'équation (E) $7x - 11y = 3$;
c) En déduire tous les couples d'entiers relatifs solutions de (E) .

Exercice n°7 :

a) Déterminer tous les couples (x , y) d'entiers relatifs vérifiant $11x - 24y = 0$.
b) Déterminer tous les couples d'entiers relatifs solutions de (E) $11x - 24y = 1$.

Exercice n°8 :

Déterminer tous les couples (x , y) d'entiers relatifs tels que $126x - 308y = 28$ (E).

Exercice n°9 :

1) Monrer que , pour tout entier relatif n , les entiers $14n + 3$ et $5n + 1$ sont premiers entre eux .
2) On considère l'équation (E) : $87x + 31y = 2$ où x et y sont des entiers relatifs :

a) Vérifier ,en utilisant la question 1) que 87 et 31 sont premiers entre eux .
En déduire un couple (u,v) d'entiers relatifs tels que $87u + 31v = 1$, puis une solution (x_0, y_0) de (E) .

b) Déterminer l'ensemble des solutions de (E) dans $\mathbb{Z}^2$.

c) Application : déterminer les points de a droite D d'équation $87x - 31y - 2 = 0$ dont les coordonnées sont des entiers naturels et dont l'abscisse est comprise entre 0 et 100 .

(indication :on remarquera que le point M de coordonnées (x , y) appartient à la droite D ssi le couple (x , -y) vérifie l'équation (E).