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
.....

Démonstration : Approche :

a	b	reste	Division euclidienne de a par b	Expression des restes en fonction de a et b

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 .....

b) **Démonstration : ROC à savoir**

*) Si a et b sont premiers entre eux alors

*) Réciproque : Si $au + bv = 1$ et si d est un diviseur positif commun de a et de b alors

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

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 392 x + 33 y = 1
u= x et v= y On exprime y en fonction de x : y = ... Et on introduit cette fonction affine dans f(x) puis dans 2nd fenêtre soit déf tab : deb tbl= 0 et 2nd graph et on cherche le couple (x, y) entiers
pas = 1
On retrouve x = 8 = u et y = - 95 = v

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 divise le produit bc et si a et b sont premiers entre eux alors .....

Démonstration : **ROC à savoir**

*) Si a est premier avec b alors

*) Et si a divise bc ,

2) Conséquences :

a) Si a et b divisent un entier c alors .....
et si a et b premiers entre eux

Démonstration : Si a divise c alors .....
Si b divise c alors .....
Et si a et b premiers entre eux alors ...

b) Si un nombre premier p divise le produit ab alors p divise .....

Démonstration : Si p nombre premier divise ab :
distinguons 2 cas : *) Si p divise a alors .....
*) Si p ne divise pas a alors comme p premier , les diviseurs positifs de p sont ....
Les valeurs possibles du PGCD (a ; p) sont donc .....

c) Si un nombre premier p divise un produit qc de nombres premiers alors p est égal à .....

III -] Equations diophantiennes :

1) Définition : Soient **a et b 2 entiers**
Elles consistent à **chercher** 2 nombres **entiers** 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