CHAPITRE 3 : PGCD, Euclide, Bézout, Gauss.

[1 PGCD 2](#_Toc342394006)

[1.1 Définition du PGCD 2](#_Toc342394007)

[1.2 Détermination à l’aide de la décomposition en facteurs premiers 3](#_Toc342394008)

[1.3 Relation entre la divisibilité de a par b et le PGCD(a ; b) 3](#_Toc342394009)

[1.4 Propriété fondamentale des diviseurs communs : 4](#_Toc342394010)

[2 L’algorithme d’Euclide 6](#_Toc342394011)

[2.1 Théorème de l’algorithme d’Euclide 6](#_Toc342394012)

[2.2 Premier corollaire de l’algorithme d’Euclide 8](#_Toc342394013)

[2.3 Deuxième corollaire de l’algorithme d’Euclide 9](#_Toc342394014)

[3 Théorème de Bézout 10](#_Toc342394015)

[3.1 Nombres premiers entre eux 10](#_Toc342394016)

[3.2 Enoncé du théorème de Bézout 11](#_Toc342394017)

[3.3 Corollaire du théorème de Bézout 13](#_Toc342394018)

[3.4 CNS pour qu’une équation diophantienne *ax* + *by* = *c* ait des solutions 14](#_Toc342394019)

[*3.5* Détermination d’une solution particulière (*x*0 ; *y*0) de *ax* + *by* = *c* 15](#_Toc342394020)

[4 Théorème de Gauss 17](#_Toc342394021)

[4.1 Enoncé du théorème de Gauss 17](#_Toc342394022)

[4.2 Première corollaire du théorème de Gauss 17](#_Toc342394023)

[4.3 Deuxième corolaire du théorème de Gauss 18](#_Toc342394024)

[4.4 Troisième corolaire du théorème de Gauss 18](#_Toc342394025)

[4.5 Quatrième corolaire du théorème de Gauss 19](#_Toc342394026)

[4.6 Utilisation du théorème de Gauss pour déterminer l’ensemble des couples de solutions entières (*x* ; *y*) d’une équation diophantienne du type *ax* + *by* = 0 20](#_Toc342394027)

[4.7 Utilisation du théorème de Gauss pour déterminer l’ensemble des couples de solutions (*x* ; *y*) d’une équation du type *ax* + *by* = *c* 21](#_Toc342394028)

CHAPITRE 3 : PGCD, Euclide, Bézout, Gauss.

# PGCD

## Définition du PGCD

Soit et deux entiers relatifs *non nuls simultanément*.

L’ensemble des diviseurs communs à et admet un plus grand élément appelé le PGCD[[1]](#footnote-1) de et

***Exemples :***

* Quel est le  ?

L’ensemble des diviseurs de est

L’ensemble des diviseurs de est

L’ensemble des diviseurs communs à et est

* Soit . Quel est le  ?

L’ensemble des diviseurs de est

L’ensemble des diviseurs de est .

L’ensemble des diviseurs communs à et est

* Soit . Quel est le  ?

L’ensemble des diviseurs de est

L’ensemble des diviseurs de est .

L’ensemble des diviseurs communs à et est

* Soit . Quel est le  ?

L’ensemble des diviseurs de est

L’ensemble des diviseurs communs à et est

***Détermination à la calculatrice :***

Ces fonctions sont présentes sur les calculatrices TI82 et TI83 (touche Math NUM)

Pour le PGCD : Math NUM 9

Les arguments négatifs ne sont pas acceptés. Dans ce cas, les remplacer par leurs opposés positifs étant donné que

## Détermination à l’aide de la décomposition en facteurs premiers

Si et sont deux entiers supérieurs ou égaux à :

Le est égal au produit des facteurs premiers communs aux deux nombres, chacun étant affecté **du plus petit exposant** avec lequel il figure dans leurs décompositions :

***Exemple :***

***Recherche du par la méthode des facteurs premiers :***

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 234 | 2 |  |  |  | 84 | 2 |  |  |  |
| 117 | 3 |  |  |  | 42 | 2 |  |  |  |
| 39 | 3 |  |  |  | 21 | 3 |  |  |  |
| 13 | 13 |  |  |  | 7 | 7 |  |  |  |
| 1 |  |  | | | 1 |  |  | | |

***Démonstration du calcul du PGCD à partir des facteurs premiers :***

Soit les décompositions en facteurs premiers de et :

où sont les **premiers nombres premiers** et où sont des entiers naturels éventuellement nuls.

Tout entier diviseur commun à et a une décomposition de la forme avec vérifiant :

car divise et car divise

Si désigne le plus petit des entiers alors

Le PGCD est obtenu lorsque , , …..,

***Exemple :***

D’où :

## Relation entre la divisibilité de a par b et le PGCD(a ; b)

Soit et deux entiers naturels. Si alors

***Démonstration :***

Soit .

Si , comme , alors . Tout diviseur de est aussi un diviseur de . Le plus grand diviseur de étant lui-même, alors le plus grand diviseur commun à et est

## Propriété fondamentale des diviseurs communs :

Soit et . Si où et , alors :

**.**

Ce qui s’écrit :

***Conséquence :***

***Remarque :***

On n’a pas la condition donc n’est pas obligatoirement la relation de la division euclidienne de *a* par *b* er n’est pas obligatoirement le reste.

***Exemple :***

Soit et .

Soit l’ensemble des diviseurs communs à et .

et

Si on écrit sous la forme , on aura par exemple :

Donc ici, et

D’après la propriété fondamentale des diviseurs communs, on a :

« L’ensemble des diviseurs communs à et et l’ensemble des diviseurs communs à et **sont identiques ».**

***Illustration sur un exemple :***

Soit l’ensemble des diviseurs communs à et .

et

***Démonstration :***

Soit et . Si où et

Soit l’ensemble des diviseurs communs à et .

Soit l’ensemble des diviseurs communs à et .

Pour montrer que , on montre que si alors puis on montre que si alors .

* Si

, alors divise et donc divise .

, alors divise .

Donc divise toute combinaison linéaire de et , donc en particulier, divise .

Comme est un diviseur à la fois de et de , alors

* si

, alors divise et donc divise .

, alors divise .

Donc divise toute combinaison linéaire de et , donc en particulier, divise .

Comme est un diviseur à la fois de et de , alors

Conclusion :

L’ensemble des diviseurs **de et**  et l’ensemble des diviseurs **de et**  sont identiques, lorsqu’on a . Cela est vrai même si ce n’est pas une relation de division euclidienne.

Comme les ensembles de diviseurs sont identiques, les PGCD aussi sont identiques : .

***Remarques :***

Puisque on peut écrire :

Pour tout :

En prenant on a :

En prenant on a :

etc.

Par exemple avec ,

***Conséquence de la propriété fondamentale des diviseurs communs :***

Le PGCD de deux nombres et reste inchangé si on remplace l’un des deux nombres par exemple par la différence avec .

# L’algorithme d’Euclide

## Théorème de l’algorithme d’Euclide

et sont deux entiers naturels *non nuls* tels que .   
Soit la suite des divisions euclidiennes :

* Division de par  :
* Division de par  :
* Division de par  :
* …..
* Division de par  :

Cette suite de divisions finit par s’arrêter lorsqu’un des restes est nul.

Le ***dernier reste non nul*** **est le .**   
Au cas où, dès la première division, le reste est nul alors et .

***Remarque :*** Ce résultat permet de calculer le sous forme algorithmique. Ce processus itératif[[2]](#footnote-2) où, à chaque étape le dividende est remplacé par le diviseur et le diviseur est remplacé par le reste est appelé Algorithme d’Euclide.

***Exemple :***

Calculer **en utilisant l’algorithme d’Euclide** : .

*Réponse :*

On écrit les relations des divisions euclidiennes successives  :

Le reste est nul, donc l’algorithme s’arrête. est égal au dernier reste non nul

Donc :

***Démonstration :***

* **1ère étape : montrons qu’il existe un avant dernier reste non nul et un dernier reste nul**

Les inégalités montrent que est une suite strictement décroissante d’entiers naturels. Or, il n’y a qu’un nombre fini d’entiers entre et . Donc cette suite est finie, c'est-à-dire qu’il existe un reste nul. Donc il existe un certain entier naturel tel que et .

* **2ème étape : montrons que .**

Considérons la relation de départ . On en déduit que .  
**La propriété fondamentale des diviseurs communs** permet d’affirmer que :

et

* **3ème étape : montrons que .**

On peut appliquer ce raisonnement à chaque égalité :

* …..

Si est le dernier reste non nul (et donc ), on a, en appliquant plusieurs fois la conséquence de **la propriété fondamentale des diviseurs communs :**

* Algorithme d’Euclide en langage naturel :

**Déclaration des variables**

entier naturel

entier naturel non nul

entier naturel

**Algorithme**

reçoit

reçoit

reçoit

**Tant que** **faire**

reçoit

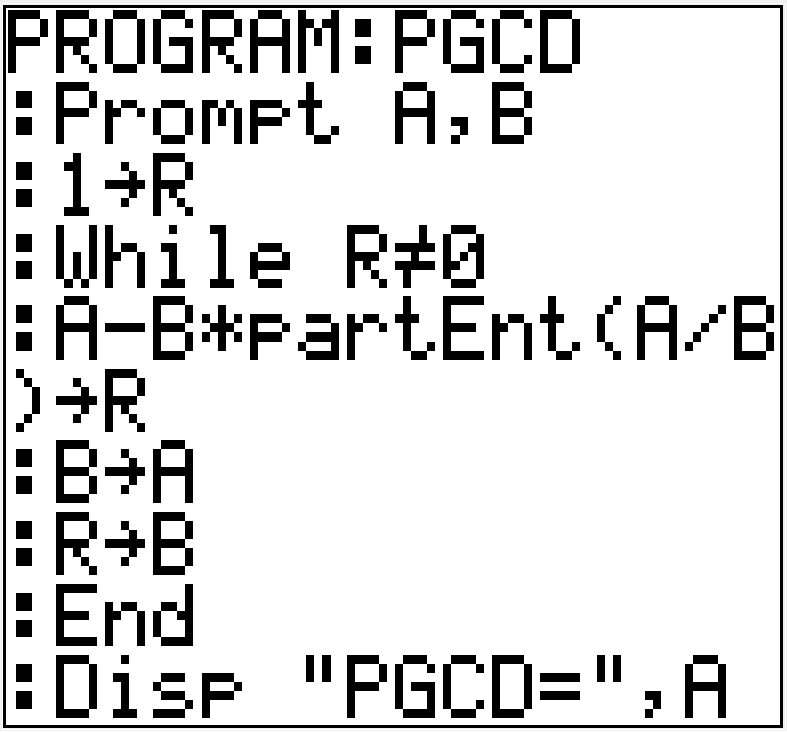
reçoit

reçoit

**Fin Tant que**

Afficher « PGCD = »,

* Algorithme d’Euclide programmé sur TI82 - 83 :



## Premier corollaire[[3]](#footnote-3) de l’algorithme d’Euclide

Soit et deux entiers naturels non nuls. Notons.

**L’ensemble des diviseurs communs à et est identique à l’ensemble des diviseurs de .**

***Illustration :***

Les diviseurs de sont 1, 2, 3, 6, 9, 13, 18, 26, 39, 78, 117, 234 et leurs opposés.

Les diviseurs de sont 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84 et leurs opposés.

Les diviseurs de sont 1, 2, 3, 6 et leurs opposés.

***Démonstration :***

On reprend les divisions euclidiennes successives présentes dans l’algorithme d’Euclide :

* …..

Si est le dernier reste non nul (et donc ), on a, en appliquant plusieurs fois **la propriété fondamentale des diviseurs communs** :

Conclusion : L’ensemble des diviseurs de est identique à l’ensemble des diviseurs communs à et

***Exemple 1 :***

Déterminer tous les diviseurs communs à de et .

*Réponse :*

On cherche à la calculatrice

On trouve

Les diviseurs de sont donc

Conclusion : Les diviseurs communs à et sont :

***Exemple 2 :***

et ont parmi leurs diviseurs communs. Donc divise

## Deuxième corollaire de l’algorithme d’Euclide

Soit et deux entiers relatifs non tous les deux nuls simultanément.

Pour tout ,

***Exemple :***

Soit et .

Prenons .

et

***Démonstration :***

On pose et .

Pour montrer que , on va montrer d’une part que divise (ce qui implique que et d’autre part que divise (ce qui implique que . Donc, au final on aura démontré que

1. **Montrons que divise**

et sont deux entiers relatifs non tous les deux nuls simultanément et .

divise à la fois et .

divise donc divise et divise donc divise

est donc un diviseur commun de et

**D’après le premier corollaire de l’algorithme d’Euclide**, l’ensemble des diviseurs communs de et est identique à l’ensemble des diviseurs de . **Donc est un diviseur de .**

1. **Montrons que divise**

On a vu dans la partie 1. Que  **divise ce qui peut se traduire** :

Il existe un entier relatif tel

divise à la fois et .

En remplaçant , on peut donc dire que  **divise à la fois et .**

D’où :

**divise à la fois et .**

**D’après le premier corollaire de l’algorithme d’Euclide**, l’ensemble des diviseurs communs de et est identique à l’ensemble des diviseurs de . Donc est un diviseur de .

D’où :

**est un diviseur de**

En remplaçant on peut donc déduire que  **est un diviseur de .**

Conclusion :

**c'est-à-dire**

# Théorème de Bézout[[4]](#footnote-4)

## Nombres premiers entre eux

***Définition :***

On dit que deux entiers relatifs *non nuls* et sont premiers entre eux (ou « étrangers ») lorsque leur PGCD est égal à .

***Remarques :***

et sont non nuls, alors :

* Les fractions et sont irréductibles lorsque et sont premiers entre eux.
* Si et ne sont pas premiers entre eux, alors on réduit ces fractions en divisant le numérateur et le dénominateur par .

***Exemple :***

Les fractions et sont irréductibles car et

***Propriété***

Soit et deux entiers naturels non nuls. On note

Soit les entiers et tels que :

Alors et sont premiers entre eux.

***Démonstration :***

divise et . Donc il existe deux entiers et dans tels que et .

Or en utilisant le deuxième corollaire de l’algorithme d’Euclide,

Donc

Conclusion :

et sont premiers entre eux.

***Exemple :***

Soit et .

et sont premiers entre eux.

## Enoncé du théorème de Bézout

On note des entiers relatifs.

Ou encore :

***Démonstration :***

*1. Démonstration de la proposition directe :*

* **Si** alors au moins un des deux entiers et est non nul. Appelons l’entier non nul.

et étant donnés, notons l’ensemble des entiers . L’ensemble  **n’est pas vide** et il **contient au moins un entier strictement positif** (l’entier qui correspond au couple ou l’entier qui correspond au couple ).

Notons  **le plus petit des entiers strictement positifs** contenus dans l’ensemble .

Il existe donc au moins **un couple d’entiers relatifs particulier**  tel que .

* Ecrivons la relation de la division euclidienne de par :
* Montrons que

Or,

donc

est une combinaison linéaire entière de et de la forme (il suffit de poser et donc .

* Montrons que divise

La condition dans la division euclidienne de par donne deux cas :

1er cas :

est de la forme «  » et donc . Mais il y a une contradiction entre et ( ne peut pas être à la fois dans un ensemble et être strictement inférieur à son plus petit élément strictement positif).

2ème cas : C’est la seule possibilité restante. Elle est donc vraie.

Conclusion : . Donc est un diviseur de .

* De la même façon, en écrivant la relation de la division euclidienne de 𝑏 par et en montrant que le reste ne peut être que nul, on montre que divise .
* Concluons que

est donc un diviseur commun de et . Or et sont premiers entre eux et n’ont donc que deux diviseurs communs et - . Comme est strictement positif, on a donc

Conclusion : **Si** alors il existe donc au moins **un couple d’entiers relatifs particulier**  tel que .

*2. Démonstration de la proposition réciproque :*

S**’il** existe au moins un couple d’entiers relatifs tel que alors, puisque tout diviseur commun à et divise la combinaison linéaire , alors tout diviseur commun à et divise 1.

Donc tout diviseur commun à et est dans l’ensemble .

D’où .

Conclusion : **S’i**l existe au moins **un couple d’entiers relatifs particulier**  tel que alors

***Exemple 1 :***

**Peut-on trouver un couple (au moins) d’entiers relatifs tel que**

*Réponse :*  et sont premiers entre eux. Donc, d’après le théorème de Bézout, il existe au moins un couple d’entiers relatifs tel que

Par exemple on trouve comme solutions.

***Exemple 2 :***

**Peut-on trouver un couple (au moins) d’entiers relatifs tel que**

*Réponse :*  et ne sont pas premiers entre eux puisque . Donc, d’après le théorème de Bézout, la réponse est non.

***Exemple 3 :***

**Soit et deux entiers relatifs. Sachant qu’il existe un couple (au moins) d’entiers relatifs tel que , que peut-on dire de et ?**

*Réponse : ,* , et sont des entiers relatifs. Donc et sont des entiers relatifs. Donc, d’après le théorème de Bézout, les entiers et sont premiers entre eux.

***Exemple 4 :***

**Montrer que pour tout , et sont premiers entre eux.**

*Réponse :* Comme la démonstration doit être faite quel que soit , on cherche une combinaison linéaire qui élimine  :

.

D’après le théorème de Bézout, comme il existe au moins un couple d’entiers relatifs non nuls tel que alors et sont premiers entre eux .

## Corollaire du théorème de Bézout

On note des entiers relatifs non nuls quelconques.

**est fausse**

Mais **est vraie**

**L’égalité est appelée « identité de Bézout ».**

***Exemple :***

Soit , .

est une identité de Bézout. Alors elle a des solutions comme par exemple : , ou etc. Mais a aussi des solutions.

***Démonstration :***

*1. Démonstration de la proposition directe :*

* **Si** alors au moins un des deux entiers et est non nul. Appelons l’entier non nul.

Notons et les entiers définis par

est non nul. De plus, d’après la propriété vue au §3.1, et sont premiers entre eux.

Donc si , alors l’équation équivaut successivement à :

avec et premiers entre eux

D’après le théorème de Bézout, cette équation a des solutions .

*2. Démonstration que la proposition réciproque est fausse :*

Si alors peut ne pas être le

Contre-exemple :

L’équation (par exemple ) alors que **n’est pas** **le PGCD** de et .

Dans le paragraphe suivant, on montre que peut être **tout multiple du**

Conclusion :

Si et sont deux entiers relatifs non nuls, alors l’équation aveca au moins un couple d’entiers relatifs et solution

## CNS[[5]](#footnote-5) pour qu’une équation diophantienne *ax* + *by* = *c* ait des solutions

On appelle équation diophantienne[[6]](#footnote-6) une équation dont les coefficients sont des entiers relatifs et dont on cherche uniquement des solutions entières relatives. L’équation est une équation diophantienne du type linéaire à deux inconnues.

L’équation où , , sont des entiers relatifs non nuls a des solutions entières relatives **si et seulement si** avec  et .

***Exemples :***

Dans le cas de et , on a

* Les équations , , … de manière générale , ont toutes une infinité de couples de solutions entières .
* Les équations , , … de manière générale avec n’ont aucun couple de solutions entières .

***Démonstration :***

**On note le**

***1ère étape : démontrons que est toujours un multiple de***

**Si**  est un couple d’entiers relatifs quelconques, puisque est un multiple de et est un multiple de **alors** avec et entiers relatifs.

. Comme est entier relatif **alors** est un multiple de .

***2ème étape : démontrons que a toujours des solutions entières relatives.***

**D**’après l’identité de Bézout, il existe au moins un couple d’entiers tels que c'est-à-dire tels que .

.

**L’identité de Bézout permet d’affirmer que l’équation** a toujours des solutions

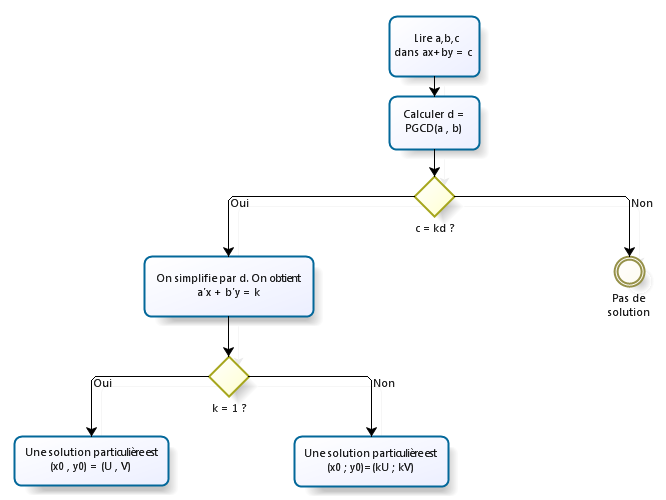
Ce sont tous les couples multiples d’un couple solution de

***Conclusion :***

Les solutions entières relatives existent **si et seulement si** l’équation est du type avec :

* est un multiple de .

## Détermination d’une solution particulière (*x*0 ; *y*0) de *ax* + *by* = *c*



Exemple :

* On calcule
* On a bien
* On divise les membres par

L’algorithme BEZOUT pour donne et

* Puisque

alors

Exemple :

* On calcule
* On a bien
* On divise les membres par

L’algorithme BEZOUT pour donne et

* Puisque

alors

Exemple :

On calcule

Donc

***Remarque :*** Comment trouver manuellement des valeurs des coefficients de Bézout et ?

Soit à trouver des valeurs de et pour l’identité de Bézout suivante

et sont premiers entre eux, donc c’est une identité de Bézout et il y a des solutions

* On pose et et on écrit la succession des divisions euclidiennes en commençant par jusqu’au dernier reste non nul
* On exprime les restes comme combinaisons linéaires de et à chaque ligne :

|  |  |  |
| --- | --- | --- |
| Avec des chiffres | Avec des lettres | **Expression du reste** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* La dernière combinaison linéaire de et est égale à . Elle donne une solution

La recherche des coefficients de Bézout peut être faite à l’aide l’algorithme « BEZOUT » suivant :

**Déclaration des variables :**

A, B, C,D,E,F, Q, R, S, T, U, V, X, Y entiers relatifs

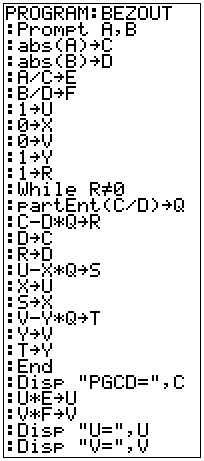
**Algorithme :**

début

Saisir

reçoit \*\*\* Cette instruction permet le fonctionnement correct si A < 0 \*\*\*

reçoit \*\*\* Cette instruction permet le fonctionnement correct si B < 0 \*\*\*

**** reçoit

reçoit

reçoit

reçoit

reçoit

reçoit

reçoit

**Tant que** **faire**

reçoit

reçoit

reçoit

reçoit

reçoit

reçoit

reçoit

reçoit

reçoit

reçoit

**FinTant que**

.

reçoit \*\*\* Cette instruction rétablit la bonne valeur de U si A < 0 \*\*\*

reçoit \*\*\* Cette instruction rétablit la bonne valeur de V si B < 0 \*\*\*

.

.

Fin

# Théorème de Gauss

## Enoncé du théorème de Gauss[[7]](#footnote-7)

Soit , , et trois entiers relatifs non nuls.

**Si** **alors**  **divise** .

***Exemple :***

**alors** divise .

***Démonstration :***

Pour démontrer le théorème de Gauss, on va utiliser le théorème de Bézout :

* et sont premiers entre eux équivaut à

a des couples d’entiers relatifs solutions.

* On multiplie les deux membres de cette égalité par  :

a des couples solutions.

* Comme divise alors il existe un entier relatif tel que et on remplace

L’égalité devient :

a des couples solutions.

a des couples solutions.

donc  **divise** .

## Première corollaire du théorème de Gauss

Soit , , et trois entiers relatifs non nuls.

**Si** **alors**  **divise** .

***Exemple :***

**alors** divise .

***Contre-exemple :***

**alors** divise est faux (car il manque l’hypothèse et sont premiers entre eux)

***Démonstration :***

* ***1ère étape : on traduit***

donc il existe et tels que

* ***2ème étape : on déduit que b divise ak***

avec donc divise

* ***3ème étape : Utilisation du théorème de Gauss***

**alors** divise .

* ***4ème étape : on traduit b divise k***

divise donc il existe tel que

Conclusion : s’écrit donc ce qui montre que divise .

## Deuxième corolaire du théorème de Gauss

Si un nombre premier divise **un produit**  alors divise au moins l’un des facteurs ou

***Exemples :***

divise . Ici divise .

divise . Ici divise et .

***Démonstration :***

Soit un nombre premier divisant le produit .

Si divise , la conclusion est assurée.

Si ne divise pas , puisque est premier, alors et sont premiers entre eux.

**Si** **alors d’après le théorème de Gauss**  **divise** .

## Troisième corolaire du théorème de Gauss

Si un nombre **premier**  divise **un produit de nombres premiers**  alors ou

***Exemples :***

divise . Ici .

divise . Ici

***Démonstration :***

Soit les nombres premiers , , .

On suppose que divise .

1er cas : . Donc divise .

2ème cas : . Donc et sont donc premiers entre eux.

**Si** **alors d’après le théorème de Gauss**  **divise** .

Et comme et sont premiers, alors .

## Quatrième corolaire du théorème de Gauss

Soit , , des entiers relatifs non nuls.

**équivaut à** et sont premiers entre eux

***Exemple :***

**équivaut à** est premier avec .

***Démonstration :***

*1. Démonstration de la proposition directe :*

Soit , , trois entiers relatifs tels que

**Supposons que et aient un diviseur commun** **entier** **naturel . Montrons qu’alors .**

divise donc divise

Comme on suppose que divise aussi et on sait (1er corollaire de l’algorithme d’Euclide) que l’ensemble des diviseurs communs à et est identique à l’ensemble des diviseurs communs de  **alors divise .**

Comme alors divise

Dans les hypothèses, donc .

**D’où divise**

Comme divise aussi , alors est un diviseur commun de et .

Dans les hypothèses**, donc .**

Le diviseur commun de et est .

Conclusion : .

*2. Démonstration de la proposition réciproque :*

Soit un nombre entier relatif premier avec le produit d’entiers relatifs .

Supposons que et aient un diviseur commun **entier** **naturel .**

Alors divise et . Comme on suppose ici que , alors .

**Comme le diviseur commun entier naturel de et est**  , on déduit que et sont premiers entre eux.

En supposons que et aient un diviseur commun **entier** **naturel , on démontre de même que et sont premiers entre eux.**

Conclusion : .

***Exemple :***

est premier avec et donc est premier avec .

Mais aussi :

est premier avec donc est premier avec chacun des facteurs et .

## Utilisation du théorème de Gauss pour déterminer l’ensemble des couples de solutions entières (*x* ; *y*) d’une équation diophantienne du type *ax* + *by* = 0

***Exemple :*** Résoudre dans l’équation

***1ère étape : on transforme l’équation en avec et premiers entre eux***

Soit et .

***2ème étape : Recherche de la forme des couples solution à l’aide du théorème de Gauss***

* **Si** vérifie alors divise
* **alors d’après le théorème de Gauss** divise .
* divise s’écrit : il existe tel que
* En reportant dans l’équation , on trouve
* **Alors** les couples solutions sont de la forme où .

***3ème étape : Réciproquement on vérifie que tout couple où est solution***

pour tout entier relatif

Conclusion : L’ensemble des solutions est

Par exemple, les couples sont des solutions.

## Utilisation du théorème de Gauss pour déterminer l’ensemble des couples de solutions (*x* ; *y*) d’une équation du type *ax* + *by* = *c*

***Rappel :***

Les solutions entières existent **si et seulement si** l’équation est du type avec :

On a vu au paragraphe 3.4 qu’on pouvait trouver un couple de solutions particulières en mettant l’équation sous la forme avec et premiers entre eux, puis en trouvant des coefficients de Bézout de l’identité de Bézout .

***Exemple 1 :***

Soit l’équation  **(E)**

1. Déterminer une solution particulière de (E)
2. Résoudre dans l’équation (E)

*Réponse :*

1. (E) est une équation du type avec et . On vérifie que et sont premiers entre eux. Donc, d’après le théorème de Bézout, cette équation admet des couples solution. A la calculatrice on trouve .

Donc une solution particulière de est :

1. *L’existence de cette solution particulière permet de revenir à une équation sans second membre comme dans l’exemple du paragraphe 4.6 précédent.*

On soustrait membre à membre (E) et

1. ***Transformation de l’équation en avec et premiers entre eux***

Soit et .

1. ***Recherche de la forme des couples solution à l’aide du théorème de Gauss***

* **Si** vérifie alors divise
* **donc d’après le théorème de Gauss** divise .
* divise s’écrit : il existe tel que
* En reportant dans l’équation ,  
  on trouve c'est-à-dire soit
* **Alors** les couples sont de la forme où .

1. ***Réciproquement on vérifie que tout couple où est solution de l’équation* (E)**

pour tout entier relatif .

Conclusion : L’ensemble des solutions de l’équation (E) est

Par exemple, les couples sont des solutions.

***Exemple 2 :***

Soit l’équation  **(E)**

1. Déterminer une solution particulière de (E)
2. Résoudre dans l’équation (E)

*Réponse :*

1. (E) est une équation du type avec et . On vérifie que et sont premiers entre eux.

Donc, (voir le schéma du § 3.5) on résout d’abord l’équation D’après le théorème de Bézout, cette équation admet des couples solution. A la calculatrice on trouve .

Donc une solution particulière de est :

1. *L’existence de cette solution particulière permet de revenir à une équation sans second membre comme dans l’exemple du paragraphe 4.7 précédent.*

On soustrait membre à membre (E) et

1. ***Transformation de l’équation en avec et premiers entre eux***

Soit et .

1. ***Recherche de la forme des couples solution à l’aide du théorème de Gauss***

* **Si** vérifie alors divise
* **donc d’après le théorème de Gauss** divise .
* divise s’écrit : il existe tel que
* En reportant dans l’équation ,  
  on trouve c'est-à-dire soit
* **Alors** les couples sont de la forme où .

1. ***Réciproquement on vérifie que tout couple où est solution de l’équation* (E)**

pour tout entier relatif .

Conclusion : L’ensemble des solutions de l’équation (E) est

Par exemple, les couples sont des solutions.

1. **PGCD :** Plus Grand Commun Diviseur [↑](#footnote-ref-1)
2. **Processus itératif :** processus répétitif [↑](#footnote-ref-2)
3. **Corollaire :** Proposition qui se déduit immédiatement d'une proposition déjà démontrée. [↑](#footnote-ref-3)
4. **Etienne BEZOUT :** Mathématicien français 1730 – 1783. Auteur d’une théorie générale des équations algébriques (équations de la forme *P*(*x*) = 0 où *P* est un polynôme). [↑](#footnote-ref-4)
5. CNS : Condition Nécessaire et Suffisante [↑](#footnote-ref-5)
6. **Diophante d’Alexandrie :** mathématicien grec (3ème siècle après Jésus Christ). Son ouvrage « *Arithmétiques »* constituent l'apogée de l'algèbre grecque (algèbre : partie des mathématiques traitant des équations et des opérations). [↑](#footnote-ref-6)
7. **Karl Friedrich Gauss**  astronome, mathématicien et physicien allemand (Brunswick 1777 - Göttingen 1855), auteur d'importants travaux en mécanique céleste, en géodésie, sur le magnétisme, l'électromagnétisme et l'optique. Sa conception moderne de la nature abstraite des mathématiques lui permit d'étendre le champ de la théorie des nombres. [↑](#footnote-ref-7)