Chapitre 7 *PGCD, Théorèmes de Bézout et de Gauss*

I - PGCD de deux entiers relatifs

Exemple : les diviseurs dans $\mathbb{Z}$ de l'entier 6, est l'ensemble, noté $\mathcal{D}(6)$, avec : $\mathcal{D}(6)$ =

Les diviseurs dans $\mathbb{Z}$ de l'entier 15 est l'ensemble noté $\mathcal{D}(15)$, avec $\mathcal{D}(15)$ =

Quels sont les diviseurs communs à 6 et 15 ?

Quel est le plus grand des diviseurs communs à 6 et 15 ?

Propriété et définition

Soit a et b deux entiers relatifs non tous les deux nuls (*i.e.* $(a\ ;\ b) \neq (0\ ;0)$).

L'ensemble des diviseurs communs à a et b admet un plus grand élément qu'on appelle le Plus Grand Commun Diviseur de a et b, et que l'on note $\boldsymbol{PGCD(a\ ;\ b)}$ ou encore $\boldsymbol{a \wedge b}$: $\boldsymbol{PGCD(a\ ;\ b)} \in \mathbb{N}$

Preuve : Soit $\mathcal{D}^+(a)$ l'ensemble formé par les entiers naturels qui divisent l'entier a, et $\mathcal{D}^+(b)$ l'ensemble formé par les entiers naturels qui divisent b.

$\mathcal{D}^+(a)$ est un ensemble non vide (car il contient l'élément 1), $\mathcal{D}^+(a)$ est un ensemble inclus dans $\mathbb{N}$, et $\mathcal{D}^+(a)$ est un ensemble fini vu qu'un entier non nul admet un nombre fini de diviseurs. De même pour $\mathcal{D}^+(b)$.

Enfin l'ensemble $\mathcal{D}^+(a) \cap \mathcal{D}^+(b)$ est non vide (contient 1), inclus dans $\mathbb{N}$ et est lui aussi fini car contenu dans deux ensembles finis. En se souvenant que toute partie non vide et finie de $\mathbb{N}$ admet un plus grand élément, il existe donc un unique élément d appartenant à $\mathcal{D}^+(a) \cap \mathcal{D}^+(b)$: d est donc le diviseur commun à a et b le plus grand possible : c'est le plus grand commun diviseur de a et b.

✂----------

Exemples

PGCD(30 ; 42) = ; PGCD(25 ; 12) =

Remarque : $\boldsymbol{PGCD\ (a\ ;\ b) = PGCD(b\ ;\ a) = PGCD\ (|a|\ ;\ |b|)}$.

On peut donc toujours se ramener au cas où a et b sont des entiers naturels.

$\boldsymbol{PGCD\ (1\ ;\ a)}$ = ….. et si $a \neq 0$, $\boldsymbol{PGCD\ (0\ ;\ a)}$ = …….

La calculatrice permet de calculer "*bestialement*" le *PGCD* de deux entiers non nuls : par exemple, pour déterminer PGCD(1544 ; 266) on tape sur *TI* : touche *math* puis flèche à droite une fois : *NBRE* puis 9 : *pgcd*(1544 ; 266).

Définition

Deux entiers relatifs a et b sont dits ♥***PREMIERS ENTRE-EUX*** si et seulement si $\boldsymbol{PGCD\ (a\ ;\ b) = 1}$. ♥

Exemple : On a vu plus haut que $PGCD(25\ ;\ 12) = 1$, donc les entiers 25 et 12 sont premiers entre eux.

***Propriété des diviseurs communs à deux entiers relatifs*.**

Soient a et b deux entiers relatifs, on note $\mathcal{D}(a\,;\,b)$ l'ensemble des diviseurs communs à a et b.

On a : $(i)\ \forall k\in\mathbb{Z}$, $\mathcal{D}(a\,;\,b)=\mathcal{D}(a-kb\,;\,b)$.

En particulier, $\mathcal{D}(a\,;\,b)=\mathcal{D}(a-b\,;\,b)$.

La notation $\mathcal{D}(a\,;\,b)$ n'est autre qu'une simplification de l'écriture $\mathcal{D}(a)\cap\mathcal{D}(b)$.

Preuve : Par double inclusion et similaire à déjà vu au chapitre 1 d'arithmétique.

✂----------

Exemple : Déterminer $\mathcal{D}(2025\,;\,2028)$

Propriétés du PGCD de deux entiers

Soient a et b deux entiers relatifs non tous les deux nuls,

$(i)\ \forall k\in\mathbb{Z}$, $PGCD(a\,;\,b)=PGCD(a-kb\,;\,b)$ *; en particulier,* $PGCD(a\,;\,b)=PGCD(a-b\,;\,b)$.

(ii) *Si* $0<b\leq a$, *alors* ♥ $PGCD(a\,;\,b)=PGCD(b\,;\,r)$ ♥, *où r est le reste dans la division euclidienne de a par b.*

(iii) *Si b est un diviseur positif de a, alors* $PGCD(a\,;\,b)=\ldots\ldots$

Preuve :

✂----------

Exercice 1

1) Montrer que deux entiers consécutifs sont premiers entre eux.

2) Démontrer que si un entier naturel n est congru à 1 modulo 7, alors $PGCD(3n+4\,;\,4n+3)=7$.

✂----------

II –L'algorithme d'Euclide

***Propriété* : L'algorithme d'Euclide** (*pratique pour calculer rapidement le PGCD de deux entiers*)

Soient a et b deux entiers naturels non nuls tels que $a\geq b$.

- ***Si b divise a, alors PGCD(a ; b) = b.***
- ***Si b ne divise pas a*** :

  On effectue la division euclidienne de a par b : il existe des entiers q_1 *et* r_1 *tels que :* $a=bq_1+r_1$ *avec :* $0\leq r_1<b$.

  Si $r_1=0$, *alors* $PGCD(a\,;\,b)=\ldots\ldots$ *car* ……

  Si $r_1\neq 0$, *alors* $PGCD(a\,;\,b)=PGCD(b\,;\,r_1)$, *et on effectue la division euclidienne de b par* r_1.

  Il existe des entiers q_2 *et* r_2 *tels que :* $b=r_1q_2+r_2$ *avec :* $0\leq r_2<r_1$.

  Si $r_2=0$, *alors* $PGCD(a\,;\,b)=PGCD(b\,;\,r_1)=\ldots\ldots$ *car* ……

  Si $r_2\neq 0$, *alors* $PGCD(b\,;\,r_1)=PGCD(r_1\,;\,r_2)$, *et on effectue la division euclidienne de* r_1 *par* r_2.

  Il existe des entiers q_3 *et* r_3 *tels que :* $r_1=r_2q_3+r_3$ *avec :* $0\leq r_3<r_2$.

Cette succession de divisions euclidiennes permet ainsi de déterminer *une suite de restes* $r_1, r_2, \ldots\ldots r_n$ *avec :* $0<r_n<\ldots\ldots<r_2<r_1$. *Cette suite de restes est une suite d'entiers naturels strictement décroissante : à ce titre il va exister un reste qui sera nul.*

Notons r_n ***le dernier reste non nul.*** *On :* $PGCD(a\,;b) = PGCD(b\,;r_1)=PGCD(r_1\,;r_2) = \ldots\ldots=PGCD(r_n\,;0) = r_n$.

Ainsi, on retiendra que :

♥♥***Lorsque b divise a, PGCD(a ; b)=…..*** ♥♥

♥♥***Lorsque b ne divise pas a****, PGCD(a ; b) est le……*

……♥♥

Exemple

Déterminer *PGCD*(135 ; 72) à l'aide de l'algorithme *d'Euclide*.

Exemple

A l'aide de la calculatrice, essayer de déterminer directement avec la fonction *pgcd* :
PGCD (2^{15} ; 38789536888912). Que constatez-vous ?

Utiliser l'algorithme d'Euclide pour déterminer ce *PGCD*.

Ce simple exemple vous convainc, je l'espère, de la puissance et rapidité de cet algorithme !

Propriétés

Soient a et b deux entiers non nuls.

1) Tout diviseur commun à a et b divise $PGCD\ (a\ ;\ b)$.

2) Pour tout entier naturel k ***non nul***, $\boldsymbol{PGCD(ka\ ;\ kb) = k\times PGCD(a;\ b)}$. Cette propriété est appelée ***l'homogénéité*** du *PGCD*.

Preuve :

1) *Avec les notations de la démonstration de l'algorithme d'Euclide, on a, en notant* $D(k)$ *l'ensemble des diviseurs de l'entier* k *:*

$D(a)\cap D(b)=D(b)\cap D(r_1)=D(r_1)\cap D(r_2)=\ldots\ldots=D(r_n)\cap D(0)=D(r_n)$. Or $r_n = PGCD(a\ ;\ b)$, donc si d est un diviseur commun à a et b, c'est-à-dire si $d\in D(a)\cap D(b)$, alors $d\in D(r_n)$, donc d divise $PGCD(a\ ;\ b)$.

2) *Soit* $d=PGCD(a;\ b)$ *et* $d'=PGCD(ka;\ kb)$.

Vu que d divise a et b, l'entier kd divise les entiers ka et kb : [*en effet, il existe* $\lambda\in\mathbb{Z}$ *tel que* $a=\lambda d$, *donc* $ka = \lambda kd$ *donc kd divise ka car* λ *est entier, et même raisonnement pour kd divise kb*].

Par suite, kd est un diviseur commun aux entiers ka et kb, donc d'après le point 1) *de cette propriété, kd divise PGCD*(*ka ; kb*), *à savoir* *kd divise d'*.

Ainsi, il existe un entier ω *tel que :* $d'=\omega kd$.

De plus, d' divise ka et kb, donc ωkd(=d') est un diviseur commun de ka et kb : donc ωd divise a et b [en effet, il existe τ∈ℤ tel que ka =τ wkd, donc comme k≠0, a=τwd, donc ωd divise a et même raisonnement pour b], donc ωd divise le PGCD(a ; b) c'est-à-dire ωd divise d.

Par suite w=1, et donc, d'=kd c'est-à-dire : PGCD(ka ; kb)=kPGCD(a ; b).

Exemple

PGCD(1500 ; 2500) =

***Propriété caractéristique du PGCD* (utile en pratique)**

Soient *a* et *b* deux entiers relatifs non tous les deux nuls et *d* un entier naturel.

♥♥ $d = PGCD(a\ ;\ b) \Leftrightarrow \exists\,(a'\ ;\ b') \in \mathbb{Z}^2$ tels que : $PGCD(a'\ ;\ b') = 1$ et $\begin{cases} a = da' \\ b = db' \end{cases}$ ♥♥ .

Preuve : *Supposons que d = PGCD(a ; b). Alors, d | a et d | b, donc il existe des entiers relatifs a' et b' tels que : a=da' et b=db'.*

De plus, d=PGCD(a ; b)=PGCD(da' ; db')=d×PGCD(a' ; b') par propriété *d'homogénéité* du *PGCD*.

Vu que *a* et *b* sont non tous les deux nuls, *d*≠0, de sorte que l'égalité : *d = d×PGCD(a' ; b') implique, après simplification par d, que PGCD(a' ; b')*=1.

Réciproquement, on suppose qu'il existe des entiers relatifs a' et b' tels que : PGCD(a' ; b') = 1 et $\begin{cases} a = da' \\ b = db' \end{cases}$.

Alors, *PGCD(a ; b) = PCGD(da' ; db') = d×PGCD(a' ; b') par propriété d'homogénéité* du *PGCD*,

PGCD(a ; b)=d×1=*d* ce qui termine la démonstration.

Application :

Expliquer le résultat suivant bien connu des collégiens : pour rendre une fraction $\frac{a}{b}$ irréductible, il suffit de diviser *a* et *b* par *PGCD*(*a* ; *b*).

III- Théorèmes célèbres de l'arithmétique

A-Théorème de Bézout

***Propriété* (*appelée l'identité de Bézout*)**

Soient a et b deux entiers relatifs non tous les deux nuls, et d = PGCD(a ; b).

Il existe des entiers relatifs u et v tels que : au + bv = d : c'est l'identité de Bézout.

Cette identité de Bézout dit que le PGCD de deux entiers non tous les deux nuls est une combinaison linéaire de ces deux entiers.

Preuve : Les notations utilisées sont celles de la démonstration de l'algorithme d'Euclide.

♣ *L'idée est de fabriquer les entiers u et v, à partir des étapes de l'algorithme d'Euclide.*

De $a = bq_1 + r_1$, on déduit que : $r_1 = a - bq_1$ qui est bien de la forme $au_1 + bv_1$ avec : $u_1 = 1$ et $v_1 = -q_1$.

(u_1 et v_1 sont bien des entiers).

De la relation : $b = r_1q_2 + r_2$, on déduit que : $r_2 = b - r_1q_2 = b - (au_1 + bv_1)q_2$ qui est bien de la forme : $au_2 + bv_2$ avec : $u_2 = -u_1q_2$ et $v_2 = 1 - v_1q_2$. (u_2 et v_2 sont bien des entiers en tant que combinaisons linéaires d'entiers).

On exprime donc, de proche en proche, chaque reste r_k comme une combinaison linéaire à coefficients entiers des entiers a et b.*

Comme l'algorithme d'Euclide se termine en un nombre fini d'étapes, et que le dernier reste non nul r_n est $PGCD(a ; b)$, il en résulte que le $PGCD(a ; b)$ s'écrit comme une combinaison linéaire à coefficients entiers des entiers a et b ce qui termine la démonstration.

**Dans l'absolu, il faudrait faire une récurrence (dite forte) si l'on veut être parfaitement rigoureux. Sera vu à bac +1.*

<u>*Remarques*</u> :

La réciproque de l'identité de Bézout est fausse ! *Pour contre-exemple on peut prendre : ……*

……..

Il n'y a pas unicité du couple (u ; v) dans l'identité de Bézout.

Par exemple, avec $a = 15$ et $b = 18$ on a $d = \ldots$, et : $\ldots \times 15 + \ldots \times 18 = 3$, donc $(u ; v) = (\ldots ; \ldots)$ convient, mais on a aussi : $\ldots \times 15 + (\ldots) \times 18 = 3$, donc $(u ; v) = (\ldots ; \ldots)$ convient aussi !

Comment déterminer en pratique un couple d'entiers relatifs (u ; v) tel que au + bv = PGCD(a ; b) ?

<u>***Méthode***</u> **: *En "remontant" les étapes écrites dans l'algorithme d'Euclide.***

<u>*Exemples*</u> : *a*) Déterminer $PGCD(135 ; 245)$, puis trouver un couple d'entiers relatifs $(u ; v)$ tel que $135u + 245v = PGCD(135 ; 245)$.

b) Expliquer pourquoi l'équation : $201x + 1002y = 3$, d'inconnues x et y, admet au moins un couple de solutions entières, et déterminer un tel couple.

✂----------

<u>***Théorème de Bézout***</u> **(*fondamental pour les exercices*).**

♥♥♥♥ ***Deux entiers relatifs a et b sont premiers entre eux <u>si et seulement si</u> il existe deux entiers relatifs u et v tels que au + bv = 1.*** ♥♥♥♥

<u>*Preuve*</u> :

✂----------

<u>*Exemples*</u>

1) Démontrer que 95 et 51 sont premiers entre eux, puis déterminer deux entiers relatifs u et v tels que : $95u + 51v = 1$.

2) Retrouver, à l'aide du théorème de *Bézout*, un résultat déjà établi : deux entiers consécutifs sont premiers entre eux.

Propriété

Soit a, b et c des entiers donnés.

L'équation (#) : ax + by = c d'inconnues (x ; y) $\in \mathbb{Z}^2$ admet des solutions entières si et seulement si PGCD(a ; b) divise c.

Pourquoi ?

✂----------

1) Résoudre dans $\mathbb{Z}^2$ l'équation : $3x + 6y = 13$.

2) Dans le plan muni d'un repère, démontrer que la droite d'équation $2x + 11y - 151 = 0$ passe par au moins un point à coordonnées entières. Déterminer les coordonnées d'un tel point.

✂----------

B- Le théorème de Gauss

♥♥ Théorème de Gauss ♥♥

Soit a, b et c des entiers relatifs non nuls.

Si a | bc, et si a et b sont premiers entre eux, alors a |c.

Preuve :

✂----------

Exemple :

Remarques : Attention, il y a deux conditions à vérifier avant de pouvoir appliquer ce théorème !

💣💣 Si $a \mid bc$, il est faux de dire que $a \mid b$ ou que $a \mid c$. 💣💣

Contre-exemple : $a = 8$; $b = 4$ et $c = 18$: on a $bc = 72$, donc $8 \mid 72$, pour autant, 8 ne divise ni 4 ni 18 !

Exemples d'utilisation du théorème de Gauss :

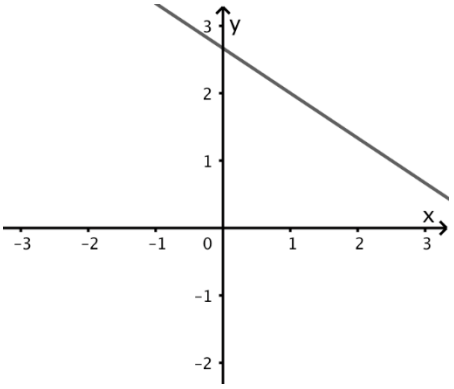
Application importante : Equations diophantiennes

Toute équation de la forme : $ax + by = c$, où *a, b et c* sont trois entiers relatifs fixés et où les inconnues *x* et *y* sont aussi deux entiers relatifs est appelée équation diophantienne.

Motivation :

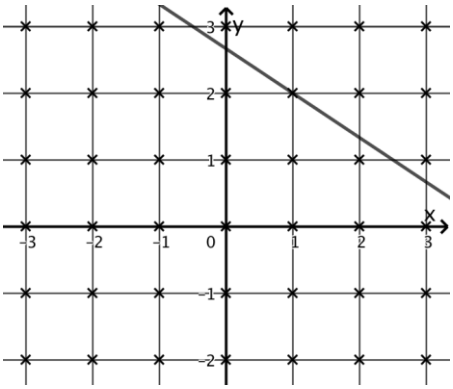
L'équation $ax + by = c$ peut être vue comme l'équation cartésienne d'une droite (dont un vecteur directeur est $\vec{u}\begin{pmatrix}-b\\a\end{pmatrix}$) dans un repère du plan. Tous les points de cette droite ont pour coordonnées un couple de nombres solution de cette équation, mais ici, nous ne cherchons que les couples de nombres entiers solution de cette équation.

Ci-contre est tracée la droite d'équation cartésienne : $2x + 3y = 8$.



Les couples de nombres entiers relatifs $(x\ ;\ y)$ peuvent être représentés dans un repère comme l'ensemble des points à coordonnées entières, c'est à dire les nœuds du quadrillage donné dans exemple ci-contre.

Résoudre dans $\mathbb{Z}^2$ l'équation diophantienne $2x + 3y = 8$ revient donc à déterminer les coordonnées des points situés sur cette droite et sur un nœud du quadrillage.



Rappelons la propriété vue en début de page 6 :

Soit a, b et c des entiers donnés.

L'équation (#) : ax + by = c d'inconnues (x ; y) $\in \mathbb{Z}^2$ ***admet des solutions entières si et seulement si PGCD(a ; b) divise c.***

On a donc une condition nécessaire et suffisante à ce que **(#)** ***ait un ensemble de solution non vide dans*** $\mathbb{Z}^2$. Voyons en pratique comment trouver l'ensemble de solution de cette équation.

Exercice 2 (*issu de texte de baccalauréat*).

On considère l'équation (E) : $7x - 6y = 1$ où x et y sont des entiers relatifs.

a) Trouver une solution particulière de (E).

b) Résoudre l'équation (E) dans $\mathbb{Z}^2$.

✂----------

Remarque : bien avoir à l'esprit que dès lors qu'on connaît une solution d'une équation diophantienne linéaire d'ordre 2, c'est le théorème de Gauss qui permet de déterminer l'expression générale de toutes les solutions de cette dernière.

Exercice 2 bis

Déterminer tous les entiers relatifs x tels que : $11x \equiv 7\ [26]$.

Exercice 3

1) Déterminer tous les couples d'entiers relatifs $(x\,;\,y)$ solutions de l'équation : $7x = 3y$.

2) Déterminer tous les couples d'entiers relatifs $(a\,;\,b)$ tels que : $15a + 19b = 7$.

En déduire tous les couples $(a\,;\,b)$ solution de cette équation avec : $0 < a < 100$, et $-30 < b < 20$.

✂----------

Exercice 4 **(*A proposer en DM*)**

Un astronome a observé un jour J_0 un corps céleste A qui apparaît périodiquement tous les 105 jours.

Six jours plus tard, (à $J_0 + 6$) il observe un autre corps céleste B dont la période d'apparition est de 81 jours.

Le but de cet exercice est de déterminer le jour J_1 de la prochaine apparition simultanée des deux objets célestes A et B aux yeux de l'astronome.

1) Soient u et v le nombre (entier) de périodes effectuées respectivement par A et B entre J_0 et J_1.

Démontrer que le couple $(u\,;\,v)$ est solution de l'équation $(E_1) : 35x - 27y = 2$.

2*a*) Déterminer un couple d'entiers relatifs $(x_0\,;\,y_0)$ solution particulière de l'équation $(E_2) : 35x - 27y = 1$.

2*b*) En déduire une solution particulière entière $(u_0\,;\,v_0)$ de (E_1).

2*c*) Déterminer toutes les solutions de (E_1).

2*d*) Quelle est la solution $(u\,;\,v)$ permettant de déterminer J_1 ?

3*a*) Combien de jours s'écouleront entre J_0 et J_1 ?

3*b*) Le jour J_0 était le mardi 7 décembre 1999. Quelle est alors la date exacte du jour J_1 ?

3*c*) Si l'astronome manque ce futur rendez-vous, combien de jours devra-t-il attendre jusqu'à la prochaine apparition simultanée des deux astres ?

✂----------

♥♥***Corollaire du théorème de Gauss***

Soit a, b et c des entiers relatifs non nuls.

♥♥***Si b et c divisent a ET si b et c sont premiers entre eux, alors bc divise a.*** ♥♥

Preuve :

✂----------

Attention, là encore, nécessité absolue d'avoir b et c premiers entre eux !

Par exemple, $6 \mid 12$ et $4 \mid 12$, pour autant, $6 \times 4 = 24$ et 24 ne divise pas 12 !

Exercice 5

1) p est entier naturel non nul, n est un entier relatif non nul, et a et b sont des entiers relatifs.

Montrer que si $na \equiv nb\ [p]$ et si $n \wedge p = 1$, alors $a \equiv b\ [p]$.

2) Résoudre l'équation suivante : $2x \equiv 6\ [13]$.

✂----------

Exercice 6

Montrer que le système de congruences suivant (inconnue $x \in \mathbb{Z}$) admet des solutions, et les déterminer toutes : $\begin{cases} x \equiv 3\ (12) \\ x \equiv 4\ (5) \end{cases}$.

✂----------

Exercice 7 **(*en vrac*)**

Soient a et b des entiers relatifs, et n un entier naturel non nul.

1) Démontrer que l'équation : $ax \equiv b\ [n]$ d'inconnue $x \in \mathbb{Z}$ admet des solutions si set seulement si $PGCD(a\ ;\ n)$ divise b.

2) CNS pour que $\sqrt{n}$ soit irrationnel.