Identité de Bezout

Created by Dhaouadi Nejib 2020

I. PGCD de deux entiers

☛ Théorème et définition

Si a et b sont deux entiers non tous nuls, alors il existe un unique entier naturel d qui vérifie les deux conditions suivantes:

- d divise a et d divise b.
- Si un entier k divise a et b alors il divise d.

L'entier d défini plus haut est noté **a∧b** et appelé **le plus grand commun diviseur de a et b**.

Conséquences

Pour tous entiers a et b non tous nuls, a∧b>0.
Pour tous entiers a et b non tous nuls, a∧b=|a|∧|b|.

L'égalité a∧b=|a|∧|b| nous permet de généraliser les propriétés du plus grand commun diviseur de deux entiers naturels non nuls à celles du plus grand commun diviseur de deux entiers non nuls.

Propriétés

Soit a et b deux entiers non tous nuls.

- Si b|a alors a∧b=|b|.
- Pour tout entier non nul a, a∧0=|a|.
- Si b ne divise pas a et si r est le reste modulo b de a alors a∧b= b∧r.
- a∧b=b∧a
- Pour tout entier non nul k, ka∧kb=|k|(a∧b).
- (a∧b)∧c=a∧(b∧c)

Exemples ✍

Cherchons 1155∧462.
On a 1155=462*2+231 donc 1155∧462=462∧231=231 car 231|462.
Cherchons 196625∧654.
Sur votre calculatrice, en tapant 196625 ab／c 654 elle affiche 300 425

654 c-à-d $\frac{196625}{654} = 300 + \frac{425}{654}$ avec 425 et 654 premiers entre eux.
Ainsi on a: 196625=654×300+425 donc 196625∧654=654∧425=1.

Calcul du PGCD: l'algorithme d'Euclide

Soit a et b deux entiers non nul.
Faisons les divisions euclidiennes successives:

$$a = bq_1 + r_1 \quad avec \quad r_1 < |b|$$
$$b = r_1q_2 + r_2 \quad avec \quad r_2 < r_1$$
$$r_1 = r_2q_3 + r_3 \quad avec \quad r_3 < r_2$$
$$r_2 = r_3q_4 + r_4 \quad avec \quad r_4 < r_3$$
$$\dots$$
$$r_{n-2} = r_{n-1}q_n + r_n \quad avec \quad r_n < r_{n-1}$$
$$r_{n-1} = r_nq_{n+1} + 0$$

On sait que:
$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = r_2 \wedge r_3 = \dots = r_{n-1} \wedge r_n$
La suite (r_n) est une suite d'entiers naturels strictement décroissante et minorée par 0 donc elle est convergente et on admet qu'elle converge vers 0 c-à-d que la suite des restes finie par un reste nul r_{n+1} et par suite r_n est le dernier reste non nul et $a \wedge b = r_{n-1} \wedge r_n = r_n$ car $r_n | r_{n-1}$

Algorithme d'Euclide

Saisir deux entiers pour trouver leur pgcd à l'aide de l'algorithme d'Euclide

196625 | 654 | Chercher

196625 = 654 × 300 + 425.
654 = 425 × 1 + 229.
425 = 229 × 1 + 196.
229 = 196 × 1 + 33.
196 = 33 × 5 + 31.
33 = 31 × 1 + 2.
31 = 2 × 15 + 1.
2 = 1 × 2 + 0.
654∧196625 = 1

Exercice 1

1) Montrer que pour tout entier n, $(5n^3 - n) \wedge (n+2) = (n+2) \wedge 38$
2) Déterminer l'ensemble des entiers n tels que :
$n+2$ divise $5n^3 - n$.

3) On pose $d = (5n^3 - n) \wedge (n+2)$.
Déterminer les valeurs possibles de d.
4) Résoudre dans $\mathbb{Z}$ l'équation : $(5n^3 - n) \wedge (n+2) = 19$

Cliquer ici pour voir les solutions

II. Entiers premiers entre eux

☛ Définition

Deux entiers a et b non tous nuls sont dits premiers entre eux, si a∧b = 1.

Exercice 2

Soit n un entier et d un entier naturel non nul.
1. Montrer que si d est un diviseur commun de n+1 et n+9 , alors d divise 8.
2. En déduire que si n est pair alors n+1 et n+9 sont premiers entre eux.

Cliquer ici pour montrer les solutions

☛ Théorème

Soit a et b deux entiers non tous nuls.
Il existe un unique couple d'entiers (a',b') tel que :
a=(a∧b)a' , b=(a∧b)b' et a'∧b' = 1.

Démonstration

Posons d=a∧b donc il existe deux entiers a' et b' tels que a=da' et b=db' et on a :
d=a∧b=da'∧db'=d(a'∧b')
donc a'∧b'=1.
Pour l'unicité, il suffit de remarquer que a=(a∧b)a'=(a∧b)a" ⇒ a'=a" car a∧b≠0 et aussi b=(a∧b)b'=(a∧b)b" ⇒ b'=b".

Exercice 3

Pour tout entier n, on pose a=n-2 et b=3n+1.
Déterminer a∧b , suivant les valeurs de n.

Cliquer ici pour voir les solutions

☛ Théorème de Gauss

Soit a, b et c trois entiers non nuls
Si a divise le produit bc avec a∧b=1 alors a divise c.

Démonstration

On a: ac∧bc=|c|(a∧b)=|c|. Or a divise bc donc il existe un entier q tel que bc=qa donc ac∧bc=ac∧qa=|a|(c∧q)=|c| ce qui prouve que a divise c.

Exercice 4

Résoudre dans $\mathbb{Z}^2$ l'équation $5x - 7y = 5$

Cliquer ici pour voir les solutions

☛ Théorème (Corollaire de Gauss)

Soit p et q deux entiers naturels non nuls et a un entier.

$$\text{Si } \begin{cases} a \equiv 0 \pmod{p} \\ a \equiv 0 \pmod{q} \\ p \wedge q = 1 \end{cases} \text{ alors } a \equiv 0 \pmod{pq}$$

Démonstration

$a \equiv 0 \pmod{p}$ ⇒a=kp et $a \equiv 0 \pmod{q}$ ⇒a=k'q donc kp=k'q alors q|kp et puisque p∧q=1 donc d'après le théorème de Gauss q|k ou encore k=k"q ce qui donne a=kp=k"qp d'où pq|a c-à-d $a \equiv 0 \pmod{pq}$

Exemple ✍

$576 \equiv 0 \pmod{9}$ et $576 \equiv 0 \pmod{16}$ (car 567=9×64) avec 16∧9=1 donc $576 \equiv 0 \pmod{9 \times 16}$ ou encore $576 \equiv 0 \pmod{144}$

Exercice 5

Montrer que pour tout entier n, $n(n+1)(n+2) \equiv 0 \pmod{6}$

Cliquer ici pour voir les solutions

III. PPCM de deux entiers

☛ Théorème et définition

Pour tous entiers a et b non nuls il existe un unique entier m strictement positif qui vérifie les deux conditions suivantes.

- m est un multiple commun 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** et est noté **a∨b** .

Conséquences

- Pour tous entiers a et b non nuls, **a∨b=|a|∨|b|**
- Pour tous entiers a et b non nuls, **(a∧b)×(a∨b)=|ab|**

Démonstration

La première conséquence est évidente en effet a∨b>0 par définition
Montrons l'égalité (a∧b)×(a∨b)=|ab|

Posons d=a∧b et m=$\frac{|ab|}{d}$
On sait qu'il existe deux entiers a' et b' tels que a=a'd et b=b'd et a'∧b'=1.
m=$\frac{|a'b'|d^2}{d}$ =d|a'b'|=|a||b'|=|b||a'| donc c'est un multiple commun de a et b.
Soit M un multiple commun de a et b, alors M=ap=bq où p et q des entiers donc a'dp=b'dq ou encore a'p=b'q on déduit alors que a' divise b'q or a'∧b'=1 donc d'après le théorème de Gauss a' divise q c-à-d q=a'k où k est un entier
Remplaçons alor q dans l'égalité M=bq on obtient M=ba'k=db'a'k donc |M|=m|k| et par suite M est un multiple de m.
En conclusion m=d|a'b'| est le ppcm de a et b et on a: md=|(da')(db')|=|ab|.

L'égalité a∨b=|a|∨|b| permet d'affirmer que les propriétés du plus petit commun multiple de deux entiers non nuls sont les mêmes que celles du plus petit commun multiple de deux entiers naturels non nuls.

Propriétés

Soit a, b et c trois entiers non nuls.

- Si b divise a alors : a∨b=|a|.

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

Exercice 6

Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ les systèmes suivants:

1) $\begin{cases} ab = -1176 \\ a \vee b = 84 \end{cases}$ 2) $\begin{cases} ab = 168 \\ a \vee b = 24 \end{cases}$

Cliquer ici pour voir les solutions

IV. Inverse modulo n

Théorème

Soit a et b deux entiers naturels non nuls tels que $b \geq 2$ et $a \wedge b = 1$.
Il existe et unique un entier u non nul inferieur à b-1 tel que
$au \equiv 1 \pmod{b}$
On dit que u est un inverse de a modulo b.

Démonstration

Soit i et j deux entiers tels que $0 \leq i < j < b$
$ia \equiv ja \pmod{b} \Leftrightarrow a(i-j) \equiv 0 \pmod{b}$ or $a \wedge b = 1$ donc b divise i-j ce qui est impossible car 0<j-i<b
Donc ia et ja ont nécessairement des restes modulo b distincts. Par suite, à chaque élément ia de {0,a,2a,...,(b-1)a}, correspond un seul reste de {0,1,...,b-1} ou encore il existe un seul entier $u \in \{0,1,...,b-1\}$ tel que
$au \equiv 1 \pmod{b}$
Il est évident que u non nul car $b \geq 2$ donc l'équalité $0 \equiv 1 \pmod{b}$ est impossible.

Exemple

Résoudre dans $\mathbb{Z}$ l'équation $3x \equiv 5 \pmod{37}$
On commence par la résolution de l'équation $3x \equiv 1 \pmod{37}$ (*)
D'après le théorème précédent, 3 et 37 sont premiers entre eux donc l'équation (*) admet une seule solution dans {1,...,36}
L'idée la plus simple est de penser à 3×12=36=37-1. Si vous pouvez penser rapidement à 3×25=75=2×37+1 ça sera mieux. Je reprend la

première idée, $3 \times 12 = 36 \equiv -1 \pmod{37} \Longrightarrow 3 \times (-12) \equiv 1 \pmod{37}$
$\Longrightarrow 3 \times (-12 + 37) \equiv 1 \pmod{37}$ ou encore $3 \times 25 \equiv 1 \pmod{37}$
Revenons à la première équation
$3x \equiv 5 \pmod{37} \Leftrightarrow 25 \times 3x \equiv 25 \times 5 \pmod{37} \Leftrightarrow x \equiv 125 \equiv 14 \pmod{37}$
alors l'ensemble des solutions est {37k+14, k∈ℤ}

Exercice 7

Montrer que les entiers 7 et 11 sont inversibles modulo 60 et déterminer leurs inverses.

Cliquer ici pour voir les solutions

Inverse modulo n

Saisir deux nombres a (a∈ℤ) et n (entier naturel non nul) pour déterminer l'inverse de a modulo n.

a: 7 n: 60 Ok

V. Identité de Bezout

☛ **Théorème** (Identité 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

On suppose que a et b sont des entiers naturels non nuls (en effet a∧b=|a|∧|b|)
Si b=1, on peut écrire 0×a+1×b=1
Si b>1, on sait qu'il existe un entier u tel que au≡1 (mod b) c-à-d au-1=kb ou encore au+(-k)b=1 avec k∈ℤ
Réciproquement: Si d est un diviseur commun de a et b alors d divise au+bv donc divise 1 alors d=1 et par suite a∧b=1.

Corollaire

Si a et b sont des entiers non nuls tels que a∧b=d alors il existe deux entiers u et v tels que **au+bv=d**

Démonstration

d=a∧b alors il existe deux entiers a' et b' tels que a=a'd , b=b'd et a'∧b'=1.
a'∧b'=1 donc d'après l'identité de Bezout il existe deu entiers u et v tels que a'u+b'v=1 et par suite da'u+db'v=d ou encore au+bv=d.

Exercice 8

1) Démontrer que 143 et 100 sont premiers entre eux.
2) Déterminer tous les couples (x,y) d'entiers tels que $143x + 100y = 1$ (E)

Cliquer ici pour voir les solutions

Algorithme d'Euclid (Etendu)

Saisir deux entiers a et b pour trouver les entiers u et v tels que au+bv=a∧b

143 | 100 | Chercher

VI. Exemples d'équations de la forme ax+by=c

Théorème

Soit a, b et c trois entiers et d=a∧b.
L'équation ax+by=c admet des solutions dans $\mathbb{Z}\times\mathbb{Z}$, si et seulement si, d divise c.

Démonstration

S'il existe un couple d'entiers (x,y) tel que ax+by=c et si d=a∧b alors d qui divise a et b divise aussi ax+by donc d divise c.
Réciproquement : si d divis c alors c=dk où k $\in\mathbb{Z}$ or d=a∧b donc d'après le corollaire de Bezout il existe un couple (u,v) d'entiers tel que au+bv=d donc a(ku)+b(kv)=dk=c et par suite l'équation ax+by=c admet des solutions.

Exemples

L'équation 10x+18y=113 n'admet aucune solution dans $\mathbb{Z}\times\mathbb{Z}$ car 10∧18=2 ne divise pas 113.
Alors que L'équation 10x+18y=112 admet des solutions dans $\mathbb{Z}\times\mathbb{Z}$ car 2 divise 112.

$10x+18y=112 \Leftrightarrow 5x+9y=56$.

Appliquons l'algorithme d'Euclid pour a=9 et b=5

$9=5\times1+4$

$5=4\times1+1$

$4=1\times4+0$

On a: $1=5-4=5-(9-5)=5\times2+9\times(-1)$

Multiplions les deux membres par 56

$5\times2+9\times(-1)=1 \Leftrightarrow 5\times112+9\times(-56)=56$ donc (112,-56) est une solution particulière de l'équation.

$5x+9y=56 \Leftrightarrow 5x+9y=5\times112+9\times(-56) \Leftrightarrow 9(y+56)=5(112-x)$. 9 divise $5(112-x)$ et $5 \wedge 9=1$ donc 9 divise 112-x ou encore $112-x=9k$, $k \in \mathbb{Z}$ ce qui donne $x=112-9k$.

Remplaçons x dans l'égalité $9(y+56)=5(112-x)$ on trouve $y=-56+5k$

Réciproquement: les valeurs trouvées $x=112-9k$ et $y=-56+5k$ vérifies bien l'équation $5x+9y=56$ en effet $5(112-9k)+9(-56+5k)=560-45k-504+45k=56$.

Conclusion: L'ensemble des solutions est $\{(112-9k,-56+5k);k \in \mathbb{Z}\}$