DEVISIBILITE DANS $\mathbb{Z}$ - IDENTITE DE BEZOUT

Résultats à retenir :

Divisibilité

1° / Soit a un entier et d un entier non nul .

On dit que d est un diviseur de a ou que a est divisible par d , s'il existe un entier q tel que a = dq .

2°/ Soit d un entier non nul et a un entier .

Si d divise a alors –d divise a .

Les multiples de d sont les éléments de l'ensemble $d\mathbb{Z} = \{ dq , q \in \mathbb{Z} \}$

3°/Soit a et b deux entiers non nuls et c un entier .

Si a divise b et b divise a , alors a = b ou a = -b .

Si a divise b et b divise c , alors a divise c .

Si a divise b et a divise c , alors a divise $\alpha b + \beta c$ pour tous entiers α et β .

4°/ Soit a et b deux entiers avec b non nul .

On appelle quotient de a par b l'entier q défini de la manière suivante

q est le plus grand entier inférieur ou égal à $\frac{a}{b}$ si b > 0 ,

q est le plus petit entier supérieur ou égal à $\frac{a}{b}$ si b < 0 .

5°/soit a et b deux entiers avec b non nul .

on appelle reste de a par b l'entier r tel que r = a – bq , où q est le quotient de a par b .

pour tout entier a et pour tout entier b non nul , il existe un couple unique d'entiers (q , r) tel que

$a = bq + r$ et $0 \leq r \leq |b|$.

Le reste de tout entier n dans la division euclidienne par un entier non nul b est un élément de l'ensemble $\{ 0 , 1 , 2 , ... , \leq |b| - 1 \}$.

Congruence

Soit n un entier naturel et non nul et a et b deux entiers .

1°/On dit que a est congru à b modulo n (ou a et b sont congrus modulo n) si a – b est un multiple de n . on note alors $a \equiv b$ (mod n) .

2°/ Soit n un entier naturel non nul .

Pour tout entier a , il existe un unique entier r appartenant à $\{ 0 , ..., n - 1\}$ tel que $a \equiv r$ (mod n) . On dit que r est le reste modulo n de a .

3°/Soit n un entier naturel non nul .

Deux entiers sont congrus modulo n , si et seulement si , ils ont le même reste modulo n .

4°/Soit a , b et c trois entiers et n un entier naturel non nul .

$a \equiv a$ (mod n)

Si $a \equiv b$ (mod n) alors $b \equiv a$ (mod n)

Si $a \equiv b$ (mod n) et $b \equiv c$ (mod n) , alors $a \equiv c$ (mod n) .

5°/Soit a , b , c et d quatre entiers et n un entier naturel non nul .

Si $a \equiv b$ (mod n) et si $c \equiv d$ (mod n) , alors

$a + c \equiv b + d$ (mod n) et $a \times c \equiv b \times d$ (mod n) .

Si $a \equiv b$ (mod n) alors $ha \equiv hb$ (mod n) pour tout entier h et $am \equiv bm$ (mod n) pour tout entier $m > 0$.

PGCD , PPCM de 2 entiers

1°/Si a et b sont deux entiers non nuls , alors il existe un unique entier naturel d sui 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 $\wedge$ b et appelé le plus grand commun diviseur de a et b .

Pour tous entiers a et b non nuls , a $\wedge$ b est un entiers naturel non nul .

Pour tous entiers a et b non nuls , a $\wedge$ b = $|a| \wedge |b|$

2°/ Soit a et b deux entiers non nuls .

Si b divise a alors a $\wedge$ b = $|b|$.

Si b ne divise pas a et si r est le reste modulo b de a alors a $\wedge$ b = b $\wedge$ r .

a $\wedge$ b = b $\wedge$ a .

pour tout entier non nul k , ka $\wedge$ kb = $|k|$ (a $\wedge$ b) .

a $\wedge$ (b $\wedge$ c) = (a $\wedge$ b) $\wedge$ c .

3°/ Deux entiers non nuls a et b sont dits premiers entre eux , si a $\wedge$ b = 1 .

Soit a et b deux entiers non nuls . Alors il existe un unique couple d'entiers (a',b') tel que a = (a $\wedge$ b)a' , b = (a $\wedge$ b)b' et a' $\wedge$ b' = 1 .

4°/

Lemme de Gauss : Soit a , b et c trois entiers non nuls . Si a $\wedge$ b = 1 et a divise bc alors a divise c .

Soit a et b deux entiers naturels non nuls et n un entier.

Si a $\wedge$ b = 1 , n = 0 (mod a) et n = 0 (mod b) alors n = 0 (mod ab) .

5°/ 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 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 notée $a \vee b$.

Pour tous entiers a et b non nuls , $a \vee b = |a| \vee |b|$

Pour tous entiers a et b non nuls , $(a \vee b) \times (a \wedge b) = |ab|$

6°/Soit a et b deux entiers non nuls .

Si b divise a alors $a \wedge b = |a|$

Pour tout entier non nul k , $ka \wedge kb = |k|(a \wedge b)$.

$a \wedge b = b \wedge a$.

$a \vee (b \vee c) = (a \vee b) \vee c$.

7°/ Soit a et b deux entiers naturels non nuls tels que $b \geq 2$ et $a \wedge b = 1$.

Alors il existe un unique entier non nul u appartenant à {0,1,…., b -1 } tel que $au = 1 \pmod b$. On dit que u est un inverse de a modulo b .

Théorème de Bezout

1°/ Deux entiers non nuls a et b sont premiers entre eux , si et seulement si , il existe deux entiers u et v tels que $au + bv = 1$.

2°/ Soit a et b deux entiers non nuls et $d = a \wedge b$. Alors il existe deux entiers u et v tels que $au + bv = d$.

3°/ Soit a, b et c trois entiers et $d = a \wedge b$. l'équation $ax + by = c$ admet des solutions dans $\mathbb{Z} \times \mathbb{Z}$, si et seulement si , d divise c .