Divisibilité dans Z

Soit a un entier et d un entier non nul.
On dit que d est diviseur de a ou a est divisible par d, s'il existe un entier q tel que a = dq .
Notation : $d|a \Leftrightarrow \exists q \in Z / \ a = dq$.

- *Si* $d|a$ *alors* $-d|a$

Soit a , b deux entiers non nuls et c un entier.

- *Si* $a|b$ *et* $b|a$ *alors* $a = b$ *ou* $a = -b$.
- *Si* $a|b$ *et* $b|c$ *alors* $a|c$
- *Si* $a|b$ *et* $a|c$ *alors* $a|xb + yc$ *pour touts* $x, y \in Z$

Quotient et reste

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 égale à* $\frac{a}{b}$ *si b >0*
- *q est le plus petit entier supérieur ou égale à* $\frac{a}{b}$ *si b <0*
- *On appelle reste de a par b l'entier r = a – bq*

$\exists!(q,r) \in Z \times N / a = bq + r \quad et \quad 0 \le r < |b|$

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

Congruence modulo n

Définition et notation:

Soit n un entier naturel non nul et a et b deux entiers .
**)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* $a \equiv b(\text{mod}\, n)$ *ou* $a \equiv b[n]$

**)Pour tout entier a, il existe un unique entier* $r \in \{0,1,...,n-1\}$ *tel que* $a \equiv r[n]$. *On dit que r est le reste' modulo n de a .*

Propriétés

Soient a et b deux entiers relatifs non nuls et $n \in N^*$

$a \equiv b[n] \Leftrightarrow n|a-b$

$a \equiv b[n] \Leftrightarrow a \equiv r[n]$ *et* $b \equiv r[n]$

$a \equiv a[n]$

Si $a \equiv b[n]$ *alors* $b \equiv a[n]$

Si $a \equiv b[n]$ *et* $b \equiv c[n]$ *alors* $a \equiv c[n]$

Si $a \equiv b[n]$ *et* $c \equiv d[n]$ *alors* $a + c \equiv b + d[n]$, $ac \equiv bd[n]$, $ha \equiv ha[n]\ (h \in Z)$ *et* $a^k \equiv b^k[n]\ (k \in N^*)$

Petit théorème de Fermat

Soit p un nombre premier et a un entier naturel alors : $p|a^p - a$

Exemple : *Montrer que, si* $13|n^{13}$ *alors* $13|n$.

On a : 13 est un nombre premier alors $13|n^{13} - n$ *et d'autre part on a :* $13|n^{13}$ *alors* $13|(n^{13} - (n^{13} - n)$

alors $13|n$

PGCD et PPCM

Soient a et b deux entiers relatifs non nuls.
1°)Le plus grand entier qui divise à la fois a et b s'appelle le plus grand commun diviseur ou PGCD de a et b. On le note $a \wedge b$.

Formellement : $d = a \wedge b$ *si et seulement si* $\begin{cases} d|a \text{ et } d|b \\ \forall k \in D_a \cap D_b, k|d \end{cases}$

2°)La plus petit entier strictement positif qui est à la fois multiple de a er b s'appelle le plus petit commun multiple ou PPCM de a et b. On le note $a \vee b$

Formellement : $m = a \vee b$ *si et seulement si* $\begin{cases} a|m \text{ et } b|m \\ \forall n \in M_a \cap M_b,\ m|n \end{cases}$

3°)Deux entiers relatifs non nul a et b sont premiers entre eux lorsque leur PGCD est égale à 1.

Propriétés

Soient a et b deux entiers relatifs non nuls.

- $a \wedge b > 0$
- $a \wedge b = |a| \wedge |b|$
- *Si* $b|a$ *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* $k \in Z^*$ *:* $ka \wedge kb = |k|(a \wedge b)$

- $a \vee b = |a| \vee |b|$
- $(a \wedge b) \times (a \vee b) = |ab|$
- *Si* $b|a$ *alors* $a \vee b = |a|$
- *Pour tout* $k \in Z^*$ *:* $ka \vee kb = |k|(a \vee b)$
- $a \vee b = b \vee a$

Théorème

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* $a' \wedge b' = 1$

Lemme de Gausse

Soit a, b et c trois entiers non nuls. Si $\begin{cases} a \wedge b = 1 \\ a|bc \end{cases}$ *alors* $a|c$

Identité de Bézout

Soit a et b deux entiers non nuls

**) $a \wedge b = 1$ si et seulement si, il existe deux entiers u et v tels que $au + bv = 1$*

**)Soit $d = a \wedge b$, alors il existe deux entiers u et v tels que $au + bv = d$*

Equations de la forme : ax+ by = c.

Soit, a, b et c trois entiers et $d = a \wedge b$.

L'équation $ax + by = c$ *admet des solutions dans* $Z \times Z$ *, si et seulement si d divise c.*