Divisibilité et nombres premiers

On dit que a divise b, ou que b est divisible par a ou bien encore que a est un multiple de b et l'on note $a \mid b$

$a \mid b \Leftrightarrow \exists c / a = b \times c$

Propriétés : $(\forall a \in \mathbb{Z}\ ; \forall b \in \mathbb{Z}\ )$

- $\left(\forall a \in \mathbb{Z}^*\ \right)\ ;\ 0 \mid a$
- *Si* $a \mid b$ *, alors* $|a| \leq |b|$.
- *Si* $a \mid b$ *et si* $b \mid a$ *alors* $a = \pm b$
- *Si* $a \mid b$ *et si* $b \mid c$ *, alors* $a \mid c$
- *Si* $a \mid b$ *et si* $a \mid c$ *, alors :* $a \mid b + c$; $a \mid b - c$ *et* $(\forall x \in \mathbb{Z}\ ; \forall y \in \mathbb{Z}\ )$; $a \mid xb + yc$
- *Si* $a \mid b$ *alors* $a \times c \mid b \times c$

définition :

Un entier n supérieur ou égal à 2 *est dit premier s'il n'admet pas dans* $\mathbb{N}$ *d'autres diviseurs que lui-même ou l'unité. Liste des nombres premiers :* $2;3;5;7;11;13;17;19;23;29;31;37;41;43...$

Théorème fondamental d'arithmétique :

Décomposition

Soit n un entier quelconque. n se décompose de manière unique à l'ordre près sous forme de produit de nombres premiers : $n = p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \times ..... \times p_r^{a_r} = \prod_{i=1}^{r} p_i^{a_i}$.

Division Euclidienne

a et b sont deux relatifs. Alors il existe un unique relatif q et un unique entier r tels que : $a=b \times q+r$ *et* $0 \leq r < |b|$

q est le quotient ; r est le reste Attention ;
Que l'on soit dans $\mathbb{Z}$ *ou* $\mathbb{N}$ *, le reste est toujours positif ou nul .*

Congruences

On dit que 2 *entiers relatifs sont congrus modulo n s'ils ont même reste dans la division par n.*
On note : $a \equiv b[n] \Leftrightarrow a - b \equiv 0[n] \Leftrightarrow \exists k \in \mathbb{Z}\ / a - b = k \times n$

Propriétés

Si $a \equiv b[n]$ *et* $a' \equiv b'[n]$

- $a + a' \equiv b + b'[n]$
- $a \times a' \equiv b \times b'[n]$
- $a^p \equiv b^p [n]$

PGCD et PPCM

Soient a et b 2 entiers relatifs. L'ensemble des diviseurs communs à a et à b admet un plus grand élément nommé le $pgcd(a;b)$. *On note aussi :* $(a \wedge b)$.

Propriétés

Si k divise a et b

- $\left(\frac{a}{k} \wedge \frac{b}{k}\right) = \frac{1}{k}(a \wedge b)$
- $(k \times a \wedge k \times b) = k \times (a \wedge b)$

On peut trouver pgcd de 3 manières

- *par décomposition des 2 nombres*
- *par une suite de divisions euclidiennes, le dernier reste non nul étant le pgcd*
- *par le théorème de Bézout Soient a et b 2 entiers relatifs.*

L'ensemble des multiples communs à a et à b admet un plus petit élément nommé le $ppcm(a;b)$.

On note aussi : $(a \vee b)$; $a \times b = pgcd(a;b) \times ppcm(a;b)$

Théorème de Bezout

Soit d le $pgcd(a;b)$; *alors, il existe 2 relatifs u et v tels que :* $a \times u + b \times v = d$.

Définition *:*

2 Nombres sont premiers entre eux si et seulement si leur pgcd est égal à 1.

1° ***corollaire***

$pgcd(a;b) = 1 \Leftrightarrow \exists (u;v) \in \mathbb{Z}^2 \ / \ a \times u + b \times v = 1$

2° ***corollaire***

$$pgcd(a;b) = 1 \Leftrightarrow \begin{cases} a = a' \times d \\ b = b' \times d \\ \exists (u;v) \in \mathbb{Z}^2 \ / \ a' \times u + b' \times v = 1 \end{cases}$$

Théorème de Gauss

Si a divise $b \times c$ *et si* $(a \wedge b = 1)$, *alors a divise c.*

Corollaire *:*

p un nombre premier divise un produit de facteurs si et seulement si il divise l'un de ces facteurs.

En particulier, si p divise a^k , *alors p divise a .*

Corollaire *:*

Si a divise c et b divise c, si $(a \wedge b = 1)$, *alors* $a \times b$ *divise c.*

***Résolution d'une équation de type**: $ax+by=c$*

Les équations de la forme (E) : $ax+by=c$ où a ;b et c sont dans $\mathbb{Z}$ se résolvent de la façon suivante:

• Si a et b sont premiers entre eux, on cherche une solution particulière $(x_0;\ y_0)$. Toute autre solution $(x;\ y)$ doit alors vérifier : $a(x-x_0)+b(y-y_0)=0$ donc : $a(x-x_0)=b(y_0-y)$.

Comme a et b sont premiers entre eux, cette dernière relation implique (d'après le Théorème de Gauss) que a divise (y_0-y) donc qu'il existe un entier k dans $\mathbb{Z}$ tel que $(y_0-y)=ka$.

En remplaçant dans l'équation précédente, on obtient alors $a(x-x_0)=b\times ka$ d'où $(x-x_0)=kb$.

Toute solution est donc de la forme : $(x=x_0+kb;\ y=y_0-ka)$;où k est un entier relatif

On vérifie alors sans problème que ces couples sont bien des solutions.

***CONCLUSION**:*

Les solutions de (E) sont les couples $(x=x_0+kb;\ y=y_0-ka)$ où $(x_0;\ y_0)$ est une solution particulière de (E) et k un entier relatif quelconque.

Pour déterminer un couple particulier de solution, on utilise, par exemple, l'Algorithme d'Euclide qui permet de déterminer un couple $(u;\ v)$ dans $\mathbb{Z}$ tel que : $au+bv=1$.

On sait qu'un tel couple existe si a et b sont premiers entre eux.

Le couple $(cu;\ cv)$ est alors une solution particulière de (E).

• Si a et b ne sont pas premiers entre eux, alors si d est le PGCD de a et b, et si d ne divise pas c alors l'équation (E) n'admet aucune solution dans Z^2.

Si d divise c, on sait alors qu'il existe A, B et C tels que $a=Ad$, $b=Bd$ et $c=Cd$ où A et B sont premiers entre eux. L'équation (E) s'écrit alors : $Ax+By=C$. On est alors dans le cas précédent.