<u>Divisibilité</u>

Définition

Soient a et b deux **entiers** relatifs. Dire que b divise a signifie qu'il existe un **entier** relatif a tel que $a = b \times a$. Pour « b divise a » on peut dire aussi « b est un diviseur a » ou bien « a est un multiple de b ».

Propriétés

La divisibilité est **transitive** c'est-à-dire que si b divise a et si a divise c alors b divise c. Cependant elle n'est pas **commutative** c'est-à-dire que si b divise a en étant distinct de a alors a ne peut pas diviser b. En effet pour qu'un nombre divise un autre nombre il est nécessaire que le premier soit **inférieur** au second. Si le nombre b divise a et c alors, pour tout entier relatif b et b, le nombre b divise b d

Division euclidienne

Soient a et b deux entiers relatifs tels que b > 0. Il existe un unique couple (q;r) d'entiers relatifs tels que $a = b \times q + r$ avec $0 \le r < b$. Effectuer la division euclidienne de a par b revient à déterminer le couple (q;r). Dans cette division, le nombre a est le **dividende**, le nombre b est le **diviseur**, le nombre a est le **quotient**, le nombre a est le **reste**. La condition a0 est le quotient que le reste doit être strictement inférieur au diviseur.

Plus grand commun diviseur

Définition

Deux entiers naturels non nuls ont toujours un **nombre fini** de diviseurs et donc un nombre fini de **diviseurs communs** (1 et -1 en font partie). Par conséquent, il existe un diviseur commun à ces deux nombres **plus grand** que les autres. Ce nombre est appelé le plus grand commun dénominateur de a et de b et sera noté PGCD(a;b).

<u>Propriétés</u>

$$PGCD(a;b) = PGCD(b;a)$$
 $PGCD(a;b) \le a$ $PGCD(a;b) \le b$ $PGCD(a;1) = 1$ $PGCD(a;a) = a$ Si b divise a alors $PGCD(a;b) = b$

Soient a et b deux entiers naturels non nuls. Soient q et r deux entiers naturels tels que $a = b \times q + r$ avec 0 < r < b. On a l'égalité suivante : PGCD(a;b) = PGCD(b;r).

Cette dernière propriété est à la base de l'algorithme d'Euclide qui permet le calcul du PGCD.

Cours Page 1

Nombres premiers entre eux

Définition

Soient a et b deux entiers relatifs non nuls. a et b sont **premiers entre eux** signifie que PGCD(a;b) = 1. Cela signifie qu'aucune table de multiplication ne contient à la fois l'un et l'autre, excepté la table de 1 évidemment!

<u>Propriété</u>

Soient a et b deux entiers relatifs non nuls.

Si d = PGCD(a;b) alors $\frac{a}{d}$ et $\frac{b}{d}$ sont des entiers relatifs premiers entre eux. Cela signifie qu'il existe deux entiers relatifs a' et b' premiers entre eux tels que $a = d \times a'$ et $b = d \times b'$.

Congruences

Définition

Soient a et b deux entiers relatifs. p désigne un entier naturel supérieur ou égal à 2. Dire que a et b sont **congrus modulo** p signifie qu'ils ont **le même reste** dans la division euclidienne par p. On note $a \equiv b[p]$.

Trois propriétés immédiates

- $a \equiv b[p] \Leftrightarrow b \equiv a[p]$
- $a \equiv 0[p] \Leftrightarrow a$ est divisible par p
- $a \equiv b[p] \Leftrightarrow b-a$ est un multiple de p

Une propriété évidente

La relation de congruence est **transitive**.

Cela signifie que si $a \equiv b[p]$ et que si $b \equiv c[p]$ alors $a \equiv c[p]$.

Les propriétés fondamentales

La relation de congruence est **compatible avec** les opérations d'addition, de soustraction et de multiplication. Cela signifie que si k est un relatif, si n est un naturel, si $a \equiv b[p]$ et si $c \equiv d[p]$, alors on a les égalités suivantes :

$$a+k \equiv b+k[p]$$
 $a+k \equiv b+k[p]$ $a \times k \equiv b \times k[p]$ $a^n \equiv b^n[p]$
$$a+c \equiv b+d[p]$$
 $a-c \equiv b-d[p]$ $a \times c \equiv b \times d[p]$ Non valable pour la division!

Cours Page 2