Divisibilité et congruences

I. Divisibilité et division euclidienne.

1.Divisibilité dans Z.

Définition :

a et b sont deux entiers relatifs ($b \neq 0$).

Dire que **b divise a** signifie qu'il existe un entier k tel que a=kb.

Vocabulaire : on dit alors que b est un diviseur de a ou que a est divisible par b.

On traduit aussi cette définition en disant que a est un multiple de b.

EXEMPLE :

1. $-45 = (-5) \times 9 = 5 \times (-9)$ donc - 5, 5,9 et - 9 divisent -45.
2. Les diviseurs dans $\mathbb{Z}$ du chiffre 6 sont -6;-3;-2;-1;1;2;3;6.

REMARQUE :
1 et -1 tout entier relatif n car $1 \times n = (-1) \times (-n) = n$.

2.Propriétés de la divisibilité.

Comparaison :

a et b sont deux entiers relatifs ($b \neq 0$), il résulte de la définition que :

1. Si b divise a alors - b divise a.

2. Si b divise a et si $a \neq 0$, alors $|b| \leq |a|$.

Théorème :

a et b sont deux entiers relatifs non nuls.

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

Théorème (transitivité):

Soient a,b et c sont trois entiers relatifs ($a \neq 0$, $b \neq 0$).

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

Théorème : divisibilité d'une combinaison linéaire.

Soient a, b, d sont trois entiers relatifs ($d \neq 0$).

Si d divise a et b, alors d divise tout entier $ma + nb$ $(m, n \in \mathbb{Z})$.

En particulier, d divise leur somme $a + b$ et leur différence $a - b$.

PREUVE :

Par hypothèses, on peut écrire $a = dk$ et $b = dk'$ avec k et k' entiers.

$ma + nb = mdk + ndk' = (mk + nk')d$ avec $mk + nk'$ entiers, donc d divise $ma + nb$.

3.La division euclidienne dans N.

Théorème :

a et b sont deux entiers naturels et b est non nul.Il existe un couple unique (q;r) d'entiers naturels tel que $a = bq + r$ et $0 \leq r < b$.

Définition :

a et b sont deux entiers naturels, $b \neq 0$.Effectuer la division euclidienne dans $\mathbb{N}$ de a par b, c'est déterminer le couple d'entiers naturels (q;r) tel que $a = bq + r$ et $0 \leq r < b$.

VOCABULAIRE :

a est le dividende, b est le diviseur, q est le quotient et r est le reste.

CONSÉQUENCE :

b divise a, si et seulement si, dans la division de a par b, le reste est nul.

4.La division euclidienne dans Z

Théorème : (admis)

a et b sont deux entiers relatifs avec b non nul.

Alors il existe un unique couple $(q; r)$ tel que q entier relatif et r entier naturel tel que $a = bq + r$ et $0 \leq r < |b|$.

EXEMPLE :

$a = -50, b = -3$; $-50 = -3 \times 16 - 2$.

Pour obtenir un reste positif, on écrit $-50 = -3 \times 16 - 3 + 3 - 2 = -3 \times 17 + 1$.

Ainsi $q = 17$ et $r = 1$.

II. Congruences.

1.Entiers congrus modulo m.

Définition :

m est un entier naturel non nul.

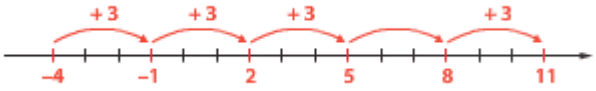
Dire que deux entiers relatifs a et b sont congrus modulo m signifie qu'ils ont le même reste dans la division euclidienne par m.

NOTATION :

On écrit $a \equiv b(mod\, m)$.On lit **a est congru à b modulo m**.

EXEMPLE :

$11 \equiv 5(mod\, 3)$ et $-4 \equiv 2(mod\, 3)$.



Théorème :

m est un entier naturel non nul.

Pour tous entiers relatifs a et b, $a \equiv b(mod\, m) \Leftrightarrow m\, divise\, a$.

REMARQUES :

1. Si r est le reste de la division euclidienne de a par m, alors $a \equiv r(mod\, m)$.
2. $a = 0(mod\, m)$ si et seulement si m divise a.

2.Propriétés des congruences.

Théorème : (transitivité)

m est un entier naturel non nul.Pour tous entier relatif a,b et c,

si $a \equiv b(mod\, m)$ et $b \equiv c(mod\, m)$, alors $a \equiv c(mod\, m)$.

Théorème : (congruences et opérations)

m est un entier naturel non nul et a,b,a',b' sont des entiers relatifs.si $a \equiv b(mod\, m)$ et $a' \equiv b'(mod\, m)$, alors :

$\star\ a + a' \equiv b + b'(mod\, m)$

$\star\ a - a' \equiv b - b'(mod\, m)$

$\star\ aa' \equiv bb'(mod\, m)$

Conséquence :

$a \equiv b(mod\, m)$, alors pour tout entier p positif, $a^p \equiv b^p(mod\, m)$.