Divisibilité et congruences

1 Divisibilité et division euclidienne

1.1 divisibilité dans $\mathbb{Z}$

Définition : Soit a et b deux entiers relatifs avec $b \neq 0$
b divise a s'il existe un entier k tel que $a = bk$

Exemple : $-63 = (-7) \times 9 = 7 \times (-9)$
donc 7 ;-7 ;-9 et 9 sont des diviseurs de 63.
Les diviseurs dans $\mathbb{Z}$ du nombre 6 sont : -6 ;-3 ;-2 ;-1 ;1 ;2 ;3 ;6
Remarque : 1 et -1 divisent tout entier relatif.

1.2 propriété de la divisibilité

Théorème :Soient a,b,d trois entiers avec $d \neq 0$
Si d divise a et b, alors d divise tout entier $ma + nb$ ($m \in \mathbb{Z}$ et $n \in \mathbb{Z}$).
En particulier, d divise leur somme $a + b$ et leur différence $a - b$.

1.3 division euclidienne dans $\mathbb{N}$

Théorème : a et b sont deux entiers naturels et $b \neq 0$.
Il existe un couple unique $(q; r)$ d'entiers naturels tels que $a = bq + r$ et $0 \leq r < b$

Démonstration :
(EXISTENCE)
Puisque $b \geq 1$, les multiples de b du type bc ($c \in \mathbb{N}$) forment une suite strictement croissante.
On note $\mathscr{E}$ l'ensemble des naturels c tels que $bc \leq a$.
$\mathscr{E}$ est une partie de $\mathbb{N}$ non vide (car $0 \in \mathscr{E}$) dont tous les termes sont majorés par a.
Théorème admis : Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.
Ainsi $\mathscr{E}$ admet un plus grand élément noté q.
bq est le plus grand multiple de b, inférieur ou égal à l'entier a.
Le multiple suivant $b(q + 1)$ est donc strictement supérieur à a.
d'où $bq \leq a < b(q + 1)$ (*)
On pose alors $r = a - bq$
Ainsi, $a = bq + r$ et d'après (*), $bq - bq \leq a - bq \leq b(q + 1) - bq$ soit $0 \leq r < b$

(UNICITE) par l'absurde
On suppose que $(q; r)$ et $(q'; r')$ sont deux couples d'entiers naturels tels que : $a = bq + r = bq' + r'$ avec $0 \leq r < b$ et $0 \leq r' < b$
Alors $r - r' = bq' - bq = b(q' - q)$ avec $q' - q$ entier, donc $r - r'$ est un multiple de b.
Or $0 \leq r < b$ et $-b < -r' \leq 0$
donc, par addition membre à membre, $-b < r - r' < b$
Le seul multiple de b dans $]-b; b[$ est 0 donc, $r - r' = 0$ soit $r = r'$
Comme $r - r' = b(q' - q)$ avec $b \neq 0$ alors $q' - q = 0$ soit $q = q'$ d'où l'unicité.

1.4 division euclidienne dans $\mathbb{Z}$

Théorème(admis) : a et b sont deux entiers relatifs (avec $b \neq 0$)
Alors il existe un unique couple $(q; r)$ avec q entier relatif et r entier naturel tel que :
$a = bq + r$ et $0 \leq r < |b|$

Exemple : division euclidienne de -50 par -3
$-50 = (-3) \times 17 + 1$ (oui)
$-50 = (-3) \times 16 - 2$ (non)

2 Congruences

2.1 entiers congrus modulo n

Définition : Soit n un entier naturel non nul Deux entiers relatifs a et b sont congrus modulo n si et seulement si ils ont le même reste dans la division euclidienne par n.
Notation : $a \equiv b \pmod{n}$

Exemple : $11 \equiv 5 \pmod{3}$

Théorème : Soit m un entier naturel non nul. Pour tout entiers relatifs a et b.
$a \equiv b \pmod{n} \Leftrightarrow$ n divise$a - b$

2.2 Propriétés des congruences

Transitivité :
Soit n un entier naturel et a,b et c des entiers relatifs.
Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$

Congruences et opérations :
Soit n un entier et a,a',b,b' des relatifs Si $a \equiv b \pmod{n}$ et $a' \equiv b' \pmod{n}$, alors : $a + a' \equiv b + b' \pmod{n}$, $a - a' \equiv b - b' \pmod{n}$, $aa' \equiv bb' \pmod{n}$