A. Ensembles $\mathbb{N}$ et $\mathbb{Z}$

L'ensemble des entiers {0 ; 1 ; 2 ; 3 ; ... } est appelé ensemble des entiers naturels et noté $\mathbb{N}$.
L'ensemble des entiers {... ; – 3 ; – 2 ; – 1 ; 0 ; 1 ; 2 ; 3 ; ... } est appelé ensemble des entiers relatifs, il est noté $\mathbb{Z}$.
Remarque : $\mathbb{N}$ est une partie de $\mathbb{Z}$: $\mathbb{N} \subset \mathbb{Z}$.
Remarque : La somme et le produit de deux entiers naturels sont des entiers naturels.
La somme et le produit de deux entiers relatifs sont des entiers relatifs.
Propriété (admise) : Toute partie non vide de $\mathbb{N}$ a un plus petit élément.
Exemples : Soit A { 8 ; 12 ; 14 ; 21 } . A est une partie de $\mathbb{N}$. Le plus petit élément de A est 8.
Soit B l'ensemble des entiers naturels impairs. B est une partie de $\mathbb{N}$. Le plus petit élément de B est 1.
Remarque : Une partie non vide de $\mathbb{Z}$ n'a pas nécessairement de plus petit élément.

B. Divisibilité

Définition : Soient a et b deux entiers relatifs. S'il existe un entier relatif k tel que $a = kb$, alors on dit que a est un multiple de b ou que b est un diviseur de a. (on dit aussi que a est divisible par b, que b divise a)

Exemple : De l'égalité $54 = 6 \times 9$, on peut déduire: 6 est un diviseur de 54, 9 est un diviseur de 54 (9 et 6 divisent 54), 54 est un multiple de 6, 54 est un multiple de 9.
Remarque : L'ensemble des multiples de 3 est l'ensemble des nombres de la forme $3k$ avec $k \in \mathbb{Z}$.

Propriétés : Soit a un entier relatif.

- 1 divise a .
- a divise a.
- Si a divise b et si b divise c alors a divise c. On dit que la relation de divisibilité est une relation transitive. On peut aussi l'énoncer : Si b est un multiple de a et si c est un multiple de b alors c est un multiple de a.
- Si a divise b alors pour tout entier m, a divise mb.
- Si a divise b et si a divise c alors a divise $b + c$ et a divise $b – c$, et plus généralement, a divise $mb + nc$ où m et n sont des entiers quelconques.
- Tout entier relatif $a \neq 0$ a un nombre fini de diviseurs.

C. Division euclidienne dans $\mathbb{N}$

Rappel : Technique de la division d'entiers naturels :
Poser la division de 43 par 5.
On peut écrire $43 = 8 \times 5 + 3$.
43 s'appelle le dividende, 5 le diviseur, 8 le quotient et 3 le reste.

43	5
3	8

Remarque : On a $3 < 5$, le reste doit toujours être strictement inférieur au diviseur.
Remarque : Les multiples de 5 sont 0, 5, 10, 15, 20, 25, 30, 35, 40, 45 et on choisit $40 = 8 \times 5$ car $45 > 43$.
Pour chercher le quotient d'une division, on cherche en pratique les multiples du diviseur et on choisit celui qui précède immédiatement le multiple supérieur au dividende.

Définition : Soit a un entier naturel et b un entier naturel non nul.
Il existe un unique couple (q ; r) d'entiers naturels tel que *:* $a = bq + r$ et $r < b$.
Le nombre a est le dividende, b le diviseur, q le quotient et r le reste.
On dit que le couple unique (q ; r) est le résultat de la division euclidienne de a par b.

Remarque : Si $r = 0$, alors est a est divisible par b.

Exemples: a) Division euclidienne de 31 par 7: $31 = 7 \times 4 + 3$.

b) Le reste de la division de a par 2 ne peut être que 0 ou 1.
Donc tout entier a peut s'écrire $2q$ ou $2q + 1$, avec $q \in \mathbb{Z}$.
Les entiers $2q$ sont les entiers pairs et les entiers $2q + 1$ sont les entiers impairs.

Remarque : Pour effectuer la division euclidienne de 1715 par 71 avec une calculatrice :
Avec une TI 89 :
Le quotient est obtenu par intDiv(1715,71) (en français divEnt(1715,71))
Le reste est obtenu par remain(1715,71) (en français reste(1715,71))
Avec une TI 82 (qui ne connaît pas la division euclidienne) :
On utilisera la fonction INT (partie entière)
Le quotient est obtenu par int (1715/71)
Une fois le quotient connu, on pourra trouver le reste
en calculant $1715 - 24 \times 71$.
Avec un tableur :
Le quotient est obtenu par ENT(1715/71) (partie entière)
Le reste est obtenu par MOD(1715; 71).

D. Division euclidienne d'un entier relatif

Soit a un entier relatif et b un entier naturel non nul.
Il existe un unique couple $(q ; r)$ tel que $a = bq + r$ et $r < |b|$.
On dit que le couple unique $(q ; r)$ est le résultat de la division euclidienne de a par b.
Le nombre a est le dividende, b le diviseur, q le quotient et r le reste.
Exemple : La division euclidienne de -514 par 35 s'écrit : $-514 = 35 \times (-15) + 11$.
Attention, dans le cas d'entiers négatifs, les fonctions des calculatrices ne donnent pas toujours les résultats attendus. Il faudra donc faire preuve de vigilance dans leur utilisation et savoir rétablir le résultat correct.

E. Congruences

Définition : Soit n un entier naturel non nul. Soient a et b deux entiers relatifs. On dit que a et b sont congrus modulo n , si et seulement si a et b ont le même reste dans la division euclidienne par n.
On dit aussi que a est congru à b modulo n .
On note cette relation $a \equiv b\ (n)$.
Propriété : $a \equiv b\ (n)$ est équivalent à $a - b$ est divisible par n.
Remarques : $a \equiv b\ (n)$ est équivalent à $b \equiv a\ (n)$.
$a \equiv 0\ (n)$ est équivalent à a est divisible par n.
Si $a \equiv r\ (n)$ et $0 \leqslant r < n$, alors r est le reste de la division euclidienne de a par n.

Propriétés :

- Si $a \equiv b\ (n)$ et si $b \equiv c\ (n)$, alors $a \equiv c\ (n)$. La relation de congruence modulo n est transitive.
- Si $a \equiv b\ (n)$ et si $a' \equiv b'\ (n)$, alors $a + b \equiv a' + b'\ (n)$ et $a - b \equiv a' - b'\ (n)$. La relation de congruence modulo n est compatible avec l'addition et la soustraction.
- Si $a \equiv b\ (n)$ et si $a' \equiv b'\ (n)$, alors $ab \equiv a'b'\ (n)$. La relation de congruence modulo n est compatible avec la multiplication.
- Si $a \equiv b\ (n)$ et $p \in \mathbb{N}^*$, alors $a^p \equiv b^p\ (n)$.

Attention, la relation de congruence n'est pas compatible avec la division ni avec la racine carrée.
Par exemple $44 \equiv 8\ (6)$, mais on ne peut pas diviser par 4 pour affirmer que 11 est congru à 2 modulo 6.
ou encore $4 \equiv 16\ (12)$, mais on ne peut pas prendre la racine carrée pour affirmer que 2 est congru à 4 modulo12.
On ne pourra en aucun cas simplifier dans une congruence comme on simplifie dans une égalité:
Une congruence du type $2a \equiv 2b\ (n)$ ne pourra pas être simplifiée par 2.