Arithmétique dans $\mathbb{Z}$

I Notations

$\mathbb{N}$ est l'ensemble des nombres entiers naturels. $\mathbb{N} = \{0;1;2;3;\cdots\cdots\}$

$\mathbb{Z}$ est l'ensemble des nombres entiers relatifs (Zahl : nombre en allemand). Il s'agit donc des entiers naturels et de leurs opposés. $\mathbb{Z} = \{\cdots;-3;-2;-1;0;1;2;3;\cdots\}$

Arithmos signifie nombre, en grec. L'arithmétique est la science des nombres entiers.

Exercice 1 :

1) Rechercher les opérations "naturelles" sur l'ensemble $\mathbb{N}$, c'est à dire les opérations dont le résultat appartient à $\mathbb{N}$. On parle de loi de composition interne.
2) Même question pour $\mathbb{Z}$.

Dans ce qui suit, on travaille, sauf indication contraire, avec des nombres entiers relatifs.

II Divisibilité dans $\mathbb{Z}$

Définition : Soit a et b deux entiers. b est un diviseur de a lorsqu'il existe un entier k tel que $a = k \times b$.
Dans ce cas, on dit que a est un multiple de b ou que b divise a et l'on note $b \mid a$.

Exemple :

- -3 divise 12 ($-3|12$) puisque $12 = -4 \times (-3)$
- -3 ne divise pas 14 ($-3 \nmid 14$)

Exercice 2 :

1) Donner l'ensemble des diviseurs de 12. On le note $D(12)$.
2) Donner l'ensemble des multiples de 7. On le note $7\,\mathbb{Z}$.

Propriétés :

- Pour tout entier n , les entiers 1, -1, n et $-n$ sont des diviseurs de n .
- Soit a et b deux entiers alors $b \mid a \Leftrightarrow (-b) \mid a \Leftrightarrow b \mid (-a) \Leftrightarrow (-b) \mid (-a)$.
- Tout entier est un diviseur de zéro. $D(0) = \mathbb{Z}$.
- Soit a et b deux entiers tels que $a \neq 0$ et $b \mid a$ alors $|b| \leqslant |a|$.
- Soit a et b deux entiers non nuls tels que $a \mid b$ et $b \mid a$ alors $a = b$ ou $a = -b$.
- Tout entier non nul n admet au plus $2n$ diviseurs compris entre $-|n|$ et $|n|$.

Démonstration 1

Exercice 3 : Déterminer les entiers n tels que $2n - 5$ divise 6.

Propriété : (transitivité de la divisibilité)
Soit a , b et c trois entiers, si c divise b et b divise a alors c divise a .

Démonstration 2

Propriété : (divisibilité d'une combinaison linéaire) Soit a , b et c trois entiers,
si c divise a et c divise b alors, quelques soient les entiers m et n, c divise $ma + nb$.

Démonstration 3

Exercice 4 : Déterminer les entiers n tels que $2n+3$ divise $n-2$.

Définition : Deux entiers sont premiers entre-eux lorsque leurs diseurs communs sont réduits à -1 et 1.

Exercice 5 : Montrer que pour tout entier n, $n+3$ et $2n+5$ sont premiers entre-eux.

III Division euclidienne

Remarque : Le mot "division" ne doit pas évoquer une opération sur $\mathbb{Z}$ puisque " $\div$ " n'est pas une loi de composition interne. ($5 \div 3 \notin \mathbb{Z}$)

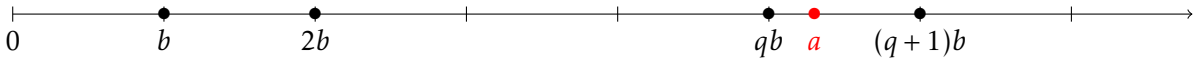
Théorème : (division euclidienne dans $\mathbb{N}$)

Soit a et b deux entiers naturels tel que $b \neq 0$.

Il existe un unique couple d'entiers naturels (q,r) tel que : $\boxed{a = bq + r}$ et $\boxed{0 \leqslant r < b}$.

Définitions : Avec les notations précédentes,

- q est appelé le quotient euclidien de la division euclidienne de a par b,
- r est appelé le reste, a le dividende et b le diviseur.



Démonstration 4

Exercice 6 : Calculer le quotient euclidien et le reste de la division euclidienne de 127 par 38.

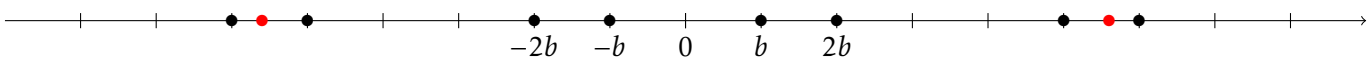
Algorithme 1 : Cet algorithme affiche la division euclidienne de l'entier naturel a par l'entier naturel b.

```
Si b = 0 alors
    Afficher "impossible"
Sinon
    q ⟵ 0
    r ⟵ a
    Tant que r ⩾ b faire
        r ⟵ r − b
        q ⟵ q + 1
    FinTantque
    Afficher a = q × b + r
FinSi
```

Théorème : (division euclidienne d'un entier relatif par un entier naturel non nul)

Soit a un entier et b un entier naturel non nul.

Il existe un unique couple d'entiers (q,r) tel que : $\boxed{a = bq + r}$ et $\boxed{0 \leqslant r < b}$.



Démonstration 5

Exercice 7 : Calculer le quotient euclidien et le reste de la division euclidienne de -102 par 7.

Exercice 8 :

1) Montrer que tout entier peut s'écrire sous la forme $2k$ ou $2k+1$ avec $k \in \mathbb{Z}$.
2) Montrer que tout entier peut s'écrire sous la forme $3k$, $3k+1$ ou $3k+2$ avec $k \in \mathbb{Z}$.

Algorithme 2 :

Écrire un algorithme qui calcule le quotient euclidien et le reste de la division euclidienne de l'entier relatif a par l'entier naturel b.

Utiliser l'algorithme 1 et distinguer les différents cas possibles suivant le signe de a.

IV Congruences

Dans cette partie, n est un entier naturel non nul.

Définition : Deux entiers a et b sont congrus modulo n lorsque les restes des divisions euclidiennes de a par n et de b par n sont égaux. On note alors $a \equiv b\,[n]$.

Exercice 9 : Montrer que -138 est congru à 12 modulo 5, mais pas modulo 8.

Propriété : Soit n un entier naturel non nul, les restes des divisions euclidiennes de a par n et de b par n sont égaux si, et seulement si, n divise $a-b$.

Démonstration 6

Corollaire : Deux entiers a et b sont congrus modulo n si, et seulement si, n divise $a-b$.

Propriété : (transitivité de la congruence) Soit a , b et c des entiers, si $a \equiv b\,[n]$ et $b \equiv c\,[n]$ alors $a \equiv c\,[n]$.

Démonstration 7

Propriété : (congruence et opérations)

Soit a ,b , a' et b' des entiers tels que $a \equiv b\,[n]$ et $a' \equiv b'\,[n]$ alors,

- $a + a' \equiv b + b'\,[n]$ *compatibilité avec l'addition*
- $a \times a' \equiv b \times b'\,[n]$ *compatibilité avec la multiplication*
- Pour tout $k \in \mathbb{N}$, $a^k \equiv b^k\,[n]$ *compatibilité avec les puissances*

Démonstration 8

Exercice 10 : Soit a, b et m des entiers.

1) Montrer que si $a \equiv b\,[n]$ alors $ma \equiv mb\,[n]$.
2) La réciproque est-elle vraie ?

Exercice 11 :

1) Déterminer le reste de la division euclidienne de 25×2^{17} par 7.
2) Déterminer les entiers k tels que $6 + k \equiv 5\,[3]$.
3) Montrer que, pour tout entier naturel k, $7^k + 3^k + 2$ est divisible par 4.

Définition : Un entier a est inversible modulo n lorsqu'il existe un entier b tel que $a \times b \equiv 1\,[n]$.

Exercice 12 :

1) Montrer que 8 et -3 sont des inverses modulo 5 mais pas modulo 4.
2) Montrer que 8 n'a pas d'inverse modulo 4.
3) Déterminer tous les inverses de 8 modulo 5.

V Mémento calculatrice

Numworks	TI 83 (82)	Casio Graph 90+E (35+E)
Menu Calculs Boîte à outils Arithmétique → *rem*(p,q) donne le reste de la division euclidienne de p par q *quo*(p,q) donne le quotient de la division euclidienne de p par q	math → NBRE (NUM) 0 : *reste*$(p;q)$ (0 : *remainder*$(p;q)$) donne le reste de la division euclidienne de p par q pour p et q positifs uniquement. 5 : *partEnt*(p/q)) donne le quotient de la division euclidienne de p par q.	MENU 1.Exe-Mat SHIFT CATALOG *MOD*(p,q) donne le reste de la division euclidienne de p par q *Int*(p/q) donne le quotient de la division euclidienne de p par q pour p et q positifs uniquement.