I DIVISION EUCLIDIENNE DANS $\mathbb{N}$:

1° Division euclidienne:

Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. On admet qu'il existe deux entiers naturels q et r tels que : $a = b\,q + r$ et $0 \leq r < b$.
On définit ainsi la « **division euclidienne dans $\mathbb{N}$** ».
Le naturel q est **le quotient** et le naturel r est **le reste** de la division euclidienne de a par b.

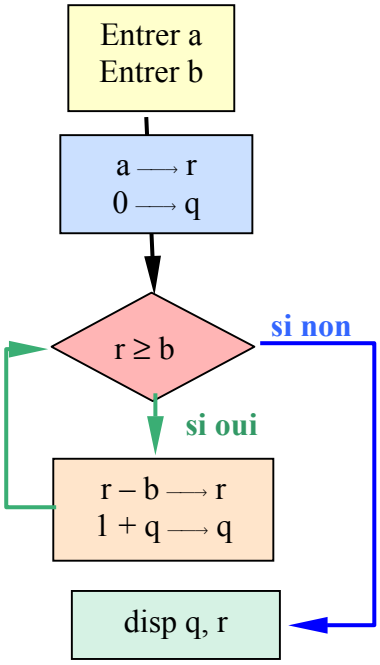
Remarque : $q \leq \frac{a}{b} < q$ on dite que q est la partie entière de $\frac{a}{b}$.

On note $q = E\left(\frac{a}{b}\right)$

Sur la calculatrice : Int (a/b)

2° Algorithme

Entrée	a un entier naturel : le dividande b entier naturel : le diviseur	input a input b
Initialisation	affecter a à r affecter 0 à q	a sto r 0 sto q
Traitement	Tant que $r \geq b$ affecter r – b à r affecter 1 + q à q	While $r \geq b$ r – b sto r 1 + q sto q end ou endW ou endWhile
Sortie	afficher q et r	disp q, r



II MULTIPLE D'UN NATUREL DANS $\mathbb{Z}$:

1° Rappels.

$\mathbb{Z}$ est l'ensemble des entiers relatifs, on dit aussi tout simplement « l'ensemble des entiers ». Il contient $\mathbb{N}$ et tous les entiers négatifs.

2° Définitions : L'entier **a est un multiple de l'entier b** signifie : il existe un entier k tel que $a = b\,k$.
On dit aussi que **b est un diviseur a**, que **a est divisible b** ou encore que **b divise a**.

Pour obtenir la liste des multiples d'un naturel dans $\mathbb{Z}$, on complète la liste des multiples d'un naturel dans $\mathbb{N}$ par celle de leurs opposés.

3°Exemple : L'ensemble des multiples de 11 dans $\mathbb{N}$ est : {0,11,22,33,… }
L'ensemble des multiples de 11 dans $\mathbb{Z}$ est : {…, –33, – 22, – 11, 0, 11, 22, 33, … } .

4° Théorème : Soit $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$
Si a et b sont des multiples de c alors a + b, a – b et, plus généralement $u \times a + v \times b$, u et v étant des entiers relatifs, sont des multiples de c.

Démonstration
a et b sont des multiples de c donc il existe deux entiers relatif q et q ' tels que : $a = c \times q$ et $b = c \times q'$

On a alors

$$\begin{cases} a + b = c \times q + c \times q' = c\,(q + q') \\ a - b = c \times q - c \times q' = c\,(q - q') \\ u \times a + v \times b = u \times c \times q + v \times c \times q' = c\,(u \times q + v \times q') \end{cases}$$

On peut donc dire que les entiers a + b, a – b et $u \times a + v \times b$ sont bien des multiples de c.

III CONGRUENCES

1° Définition congruence

Soit n un entier supérieur où égal à 2.
On dit que deux entiers a et b sont dits congrus modulo n si et seulement si a – b est un multiple de n.
On note (notation de Gauss) $a \equiv b$ (modulo n) ou $a \equiv b$ (mod n) ou $a \equiv b \ [n]$

2° Propriété

Deux entiers a et b sont dits congrus modulo n si et seulement si ils ont le même reste dans la division par n

Démonstration

Si $a \equiv b$ modulo n alors a – b s'écrit $k \times n$ où k est un entier.
Les divisions euclidiennes de a et de b par n donnent : $a = q \times n + r$ et $b = q' \times n + r'$ avec $0 \leq r < n$ et $0 \leq r' < n$
On a donc : $a - b = a \times n + r - q' \times n - r' = (q - q') \times n + r - r'$
Comme on a vu que : $a - b = k \times n$ on peut dire que $(q - q') \times n + r - r' = k \times n$ donc $r - r' = (k - q + q') \times n$.
r – r' est donc un multiple de n

$\begin{cases} 0 \leq r < n \\ 0 \leq r' < n \end{cases}$ donc $\begin{cases} 0 \leq r < n \\ -n < -r' \leq 0 \end{cases}$ donc $-n < r - r' < n$

Le seul multiple de n strictement compris entre – n et n est 0. On a donc r – r' = 0 c'est à dire r = r'
Réciproquement
Si a et b ont le même reste r dans la division par n on a :

$\begin{cases} a = q \times n + r \\ b = q' \times n + r \end{cases}$ donc $a - b = q \times n + r - q' \times n - r = (q - q') \times n$

ce qui prouve que a – b est bien un multiple de n

3° Compabilité avec l'addition.

Théorème :

Si $a \equiv b$ (mod n) et $a' \equiv b'$ (mod n) alors $a + a' \equiv b + b'$ (mod n).
En ajoutant membre à membre deux congruences modulo n, on obtient une congruence modulo n.
On dit aussi que la relation de congruence est compatible avec l'addition.

Démonstration

Si $\begin{cases} a \equiv b \ (\text{mod } n) \\ a' \equiv b' \ (\text{mod } n) \end{cases}$ alors $\begin{cases} a - b = k \times n \\ a' - b' = k' \times n \end{cases}$ où k et k' sont deux entiers.

En ajoutant membre à membre les égalités on obtient :
$a + a' - (b + b') = k \times n - k' \times n = (k - k') \times n$.
On a donc bien $a + a' \equiv b + b'$ (mod n).

4° Compabilité avec multiplication.

Théorème

Si $a \equiv b$ (mod n) et $a' \equiv b'$ (mod n) alors $a \times a' \equiv b \times b'$ (mod n).
En multipliant membre à membre deux congruences modulo n, on obtient une congruence modulo n.
La congruence est compatible avec la multiplication.

Démonstration

Si $\begin{cases} a \equiv b \ (\text{mod } n) \\ a' \equiv b' \ (\text{mod } n) \end{cases}$ alors $\begin{cases} a - b = k \times n \\ a' - b' = k' \times n \end{cases}$ où k et k' sont deux entiers.

On a :
$a \times a' - b \times b' = a \times a' - a \times b' + a \times b' - b \times b' = a\,(a' - b') + b' \times (a - b) = a \times k' \times n + b' \times k \times n$
On obtient bien un multiple de n et ion peut donc dire que : $a \times a' \equiv b \times b'$ (mod n)

Conclusion

:Soient $\begin{cases} a \equiv b \ (\text{mod } n) \\ c \equiv d \ (\text{mod } n) \\ u \text{ et } v \text{ deux entiers relatifs} \end{cases}$ alors :

$\mathbf{a + c} \equiv b + c$ (mod n)
$a - c \equiv b\text{-}d$ (mod n)
$a \times c \equiv b \times d$ (mod n)
$a \times u + c \times v \equiv b \times u + d \times v$ (mod n)
$a^k \equiv b^k$ (mod n)