Congruences :

Définition : Soit $N > 1$ un entier. Deux entiers a et b sont dits congrus modulo N si N divise $a - b$. On note

$$a \equiv b \mod N$$

(ou $a \equiv b \ [N]$)

Propriétés :

1) On a $a \equiv 0 \mod N$ si et seulement si N divise a.

2) Si $a \equiv b \mod N$ et $b \equiv c \mod N$ alors $a \equiv c \mod N$

3) On a l'équivalence :

$$a \equiv b \mod N_1 \quad a \equiv b \mod N_2 \iff a \equiv b \mod \text{ppcm}(N_1, N_2)$$

4) Tout entier est congrus modulo N à un et un unique élément de l'ensemble $\{0, 1, \dots, N-1\}$. Il s'agit précisément du reste de la division euclidienne de cet entier par N.

5) Les entiers congrus à a modulo N sont les entiers de la forme $a + kN$ pour $k \in \mathbb{Z}$.

6) Si $a \equiv a' \mod N$ et $b \equiv b' \mod N$ alors :

$$a + b \equiv a' + b' \mod N \quad \text{et} \quad ab \equiv a'b' \mod N$$

Exercice : Trouver tous les entiers tels que

$$7 \text{ divise } x^2 + x + 1$$

Théorème : Soit $N > 1$ un entier et a un entier premier avec N. Alors il existe un entier b tels que

$$ab \equiv 1 \mod N$$

un tel entier est appelé un inverse de a modulo N.

Preuve : Comme a et N sont premiers entre eux, d'après le lemme de Bézout, il existe donc entiers u et v tels que

$$au + Nv = 1$$

ainsi $ax \equiv 1 \mod N$. D

Corollaire : Soit $N > 1$ un entier et a un entier premier avec N, alors si pour deux entiers c et c' on a $ac \equiv ac' \mod N$, alors $c \equiv c' \mod N$

Chapitre : Groupes, anneaux et corps

I • Groupes :

Définition : Un groupe est la donné d'un ensemble G et d'une application

$$G \times G \longrightarrow G$$
$$(x, y) \longmapsto x * y$$

tels que $(G, *)$ vérifie les propriétés suivantes :

1) (Élément neutre) Il existe $e \in G$ tel que $\forall x \in G$,
$$e * x = x * e = x$$

2) (Associativité) Pour tout $x, y, z \in G$
$$(x * y) * z = x * (y * z)$$

3) (Élément inverse) $\forall x \in G$, $\exists x' \in G$ tels que
$$x * x' = x' * x = e$$

Si de plus $\forall x, y \in G$, $x * y = y * x$, on dit que $(G, *)$ est un groupe commutatif.

Exemples :

1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ munis de l'addition sont des groupes abéliens :

0 est l'élément neutre, l'inverse de x est $-x$

Notons que $(\mathbb{N}, +)$ n'est pas un groupe.

2) $\mathbb{Q}^*$, $\mathbb{R}^*$, et $\mathbb{C}^*$ munis de la multiplication sont des groupes:
1 est l'élément neutre, l'inverse de x est $\frac{1}{x}$.

Remarque: $\mathbb{Z}^*$ muni de la multiplication n'est pas un groupe.

Notation: Si $(G, *)$ est un groupe, on note souvent xy au lieu de $x * y$.

Proposition: Soit $(G, *)$ un groupe. On a les propriétés suivantes:
1) L'élément neutre est unique. Il est souvent noté 1.
2) L'inverse d'un élément x est unique, il est souvent noté x^{-1}.
3) L'inverse de l'inverse de x est x, i.e., $(x^{-1})^{-1} = x$
4) $(xy)^{-1} = y^{-1}x^{-1}$.

Preuve:
1) Soient e, e' deux éléments neutres.
Puisque e est un élément neutre, on a $ee' = e'e = e'$
et puisque e' est un élément neutre, on a $e'e = ee' = e$

Par conséquent, on a $e = e'$.

2) Soit $x', x'' \in G$ deux éléments tels que $x'x = xx' = e$

$x''x = xx'' = e$

alors $x''xx' = (x''x)x' = 1 \cdot x' = x'$

$= x''(xx') = x'' \cdot 1 = x''$

donc $x = x''$.

3) On a $x^{-1}x = xx^{-1} = 1$ donc x est l'inverse de x^{-1} par définition de l'inverse.

4) On a

$$(xy)\cdot(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x \cdot 1 \cdot x^{-1} = xx^{-1} = 1.$$

D'où $y^{-1}x^{-1}$ est l'inverse de xy.

Notation : Pour $n \in \mathbb{N}_{\geq 1}$, on note $x^n = \underbrace{x \cdots x}_{n \text{ fois}}$

Par convention on note $x^0 = 1$.

Sous-groupes :

Définition : On dit que H est un sous-groupe de $(G, *)$ si H est un sous-ensemble de G tels que $*$ se restreint à une application

$$H \times H \longrightarrow H$$

qui donne une loi de groupe sur H.

Ainsi un sous-groupe H stable par la loi $*$, i.e :

$$\forall x,y \in H, \quad x*y \in H$$

l'élément neutre $1 \in H$ et si $x \in H$, alors $x^{-1} \in H$.

Remarquons qu'il est inutile de vérifier l'associativité.

En fait, on peut raccourcir ces vérifications :

Proposition : Soit H un sous-ensemble d'un groupe G. Alors H est un sous groupe de G si :

1) $1 \in H$

2) $\forall x,y \in H, \quad xy^{-1} \in H$.

Preuve. Il est facile de voir que ces conditions sont nécessaires.

Réciproquement, supposons que 1) et 2) sont vérifiées et montrons que H est un sous groupe.

Si $y \in H$, $1 \cdot y^{-1} = y^{-1} \in H$, donc tout élément de H admet un inverse dans H. Soient donc $x, y \in H$, alors $y^{-1} \in H$ donc d'après 2) appliqué à x, y^{-1}, on a

$$x(y^{-1})^{-1} = xy \in H$$

donc H est stable par l'opération de groupe. ∎