I. Définition

Soit $n \geq 2$ **un entier. On dit que** a **est congru à** b **modulo** n**, si** n **divise** $b-a$**. On note alors** $a \equiv b\,[n]$**.**
On note aussi parfois $a \equiv b\,(\mathrm{mod}\ n)$ **ou** $a \equiv b\,(n)$**.**

Une autre formulation est : $a \equiv b\,(\mathrm{mod}\ n) \Leftrightarrow \exists k \in Z,\ a = b + kn$

Remarque : n **divise a si et seulement si** $a \equiv 0\,[n]$**.**

Les propriétés suivantes sont des conséquences immédiates de la définition

Propriétés
• $a \equiv a\,[n]$ **: La relation de congruence modulo** n **est réflexive ;**
• **Si** $a \equiv b\,[n]$**, alors** $b \equiv a\,[n]$ **: La relation de congruence modulo** n **est symetrique ;**
• **Si** $a \equiv b\,[n]$ **et** $b \equiv a\,[n]$**, alors** $a \equiv c\,[n]$ **: La relation de congruence modulo** n **est transitive.**
Soit n **un entier naturel non nul,** a **et** a' **deux entiers relatifs,** t **et** r' **les restes respectifs des divisions euclidiennes de** a **et** a' **par** n**.**
• **On a:** $a \equiv a'\,[n] \Leftrightarrow r = r'$
Soit n **un entier naturel non nul et** a, a', b, b' **quatre entiers relatifs.**
• **Si** $a \equiv a'\,[n]$ **et** $b \equiv b'\,[n]$ **alors** $a + b \equiv a' + b'\,[n]$**.**
• **Si** $a \equiv a'\,[n]$ **et** $b \equiv b'\,[n]$ **alors** $a \times b \equiv a' \times b'\,[n]$
On dit que la congruence modulo n **est compatible avec l'addition et la multiplication dans** Z
• **Si** k **est un entier naturel non nul, on a** $a \equiv a'\,[n] \Leftrightarrow a^k \equiv a'^k\,[n]$

II. Congruences particulières (Caractères de divisibilité)

a) Divisibilité par 2

Un entier x est divisible par 2 si et seulement si son chiffre des unités simples est pair, c'est-à-dire si l'entier x se termine par 0 ; 2 ; 4 ; 6 ou 8.

b) Divisibilité par 3 et par 9

Un entier x est divisible par 3 (respectivement par 9) si et seulement si la somme de ces chiffres est divisible par 3 (respectivement par 9).

c) Divisibilité par 5

Un entier x est divisible par 5 si et seulement il se termine par 0 ou 5.

d) Divisibilité par 11

Un entier N est divisible par 11 si et seulement si la différence de la somme des chiffres de rang pair et de la somme des chiffres de rang impair est divisible par 11.

e) Divisibilité par 4 et par 25

Un entier x est divisible par 4 (respectivement par 25) si et seulement si le nombre formé par les deux derniers chiffres est divisible par 4 (respectivement par 25).

(A démontrer dans la partie exercice)

III. Petit théorème de Fermat

Si p est un nombre premier et $a \in Z$ alors :

$$a^p \equiv a\,[p]$$

Corollaire : Si p ne divise pas a alors :

$$a^{p-1} \equiv 1\,[p]$$

p divise $C_k^p = \frac{p!}{k!(p-k)!}$ pour $1 \leq k \leq p-1$, c'est-à-dire $C_k^p \equiv 0\,[p]$

Démonstration :

En effet, $C_k^p = \frac{k!}{p!(k-r)p!}$ donc $p! = k!\,(p-k)!C_k^p$ ainsi $p|k!\,(p-k)!C_k^p$. Or comme $1 \leq k \leq p-1$ alors p ne divise pas $k!$ (sinon p divise l'un des facteurs de $k!$ or, ils sont tous supérieures à p). De même p ne divise pas $(p-k)!$ donc p devise C_k^p.

IV. Congruence et Structure d'anneau (Ensemble Z/nZ)

IV.1 Classe d'équivalence modulo n

a) Définition :

Lorsqu'un nombre quelconque n de Z est divisé par un entier naturel n, les restes possibles sont : 0, 1 , 2 ,…, n-1.

On dit qu'un élément x de Z appartient à la classe $p$modulo n : si : $x \equiv p$ avec $n - 1 \geq 0$.

D'une manière générale, si x est un élément de Z, alors la classe de x modulo n est l'ensemble de tous les éléments de Z qui ont le même reste que x dans la division par n ; on le note $cl(x) = \dot{x}$ tel que $cl(x) = \dot{x} = \{y \in Z / x - y \equiv 0\,[n]\}$

b) Ensemble quotient Z/nZ

L'ensemble des classes $p$modulo n est noté par Z/nZ et s'appelle groupe quotient de Z/nZ tel que : $Z/nZ = \{\dot{0}; \dot{1}; \dot{2}; \ldots; \dot{n-1}\}$.

IV.2) Propriétés dans Z/nZ

a) Propriétés (Addition)

1) L'associativité : $\dot{x} + (\dot{y} + \dot{z}) = (\dot{x} + \dot{y}) + \dot{z}$

2) La commutativité : $\dot{x} + \dot{y} = \dot{y} + \dot{x}$

3) L'élément neutre : $\dot{0}$ (car $\dot{x} + \dot{0} = \dot{x}$)

4) L'élément $\dot{-x}$, symétrique x

b) Propriétés (Multiplication)

1) L'associativité : $\dot{x} \times (\dot{y} \times \dot{z}) = (\dot{x} \times \dot{y}) \times \dot{z}$

2) La commutativité : $\dot{x} \times \dot{y} = \dot{y} \times \dot{x}$

3) L'élément neutre : 1

4) La distributivité par rapport à l'addition, soit : $\dot{x} \times (\dot{y} + \dot{z}) = (\dot{x} \times \dot{y}) + (\dot{x} \times \dot{z})$

On dit qu'un anneau commutatif unitaire A est intègre si pour tout x, y de A, on a : $x \times y = 0 \Rightarrow \begin{cases} x = 0 \\ y = 0 \end{cases}$

Lorsque l'anneau n'est pas intègre, il existe x et y, tous non nuls, dont le produit est zéro. On dit alors que x et y sont des diviseurs de zéro.