TS spé

Fiche sur les congruences

Pour toute la fiche, n désigne un entier naturel supérieur ou égal à 2.

I. Généralités

1°) Définition

a et b sont deux entiers relatifs.

On dit que les entiers a et b sont **« congrus modulo n »** pour exprimer que leur différence est divisible par n.

2°) Notation

On écrit : $a \equiv b \pmod{n}$.

On écrit aussi parfois $a \equiv b \ [\text{mod. } n]$ ou même $a \equiv b \ [n]$.

3°) Exemples

$23 \equiv 2 \pmod{7}$

$4 \equiv -1 \pmod{5}$

4°) Reprise de la définition

$a \equiv b$ [mod. n] $\Leftrightarrow$ $a - b$ (ou $b - a$) est divisible par n

$a \equiv b \pmod{n} \Leftrightarrow \exists k \in \mathbb{Z}$ tel que $a = b + kn$

5°) Propriété évidente

a est un entier relatif.

$a \equiv 0 \pmod{n} \Leftrightarrow a$ est divisible par n.

II. Application de la définition

1°) Propriété

Soit a un entier relatif fixé.
Les entiers relatifs congrus à a modulo n sont les entiers de la forme $a + kn \ (k \in \mathbb{Z})$.

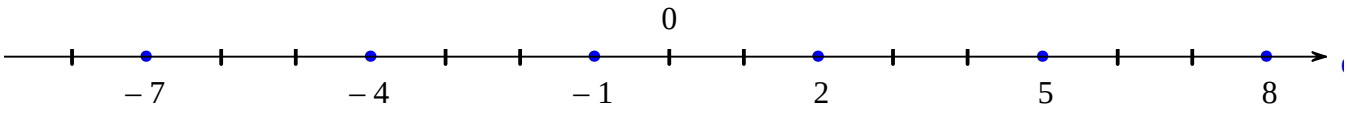
Autre formulation :

Les solutions dans $\mathbb{Z}$ de l'équation $x \equiv a \pmod{n}$ sont les entiers relatifs de la forme $a + kn \ (k \in \mathbb{Z})$.

2°) Exemple

Les entiers relatifs congrus à – 1 modulo 3 sont les entiers de la forme $3k-1$ $(k \in \mathbb{Z})$.

Il est intéressant de les représenter sur la droite réelle (droite graduée).



On note *E* l'ensemble des entiers relatifs congrus à – 1 modulo 3.
E est l'ensemble des entiers de la forme $3k-1$ $(k \in \mathbb{Z})$.
C'est aussi l'ensemble des entiers de la forme $3k+2$ $(k \in \mathbb{Z})$ ou encore l'ensemble des entiers de la forme $3k+5$ $(k \in \mathbb{Z})$.
On peut en fait remplacer – 1 par n'importe quel élément de *E*.

3°) Propriété

Soit *b* un entier quelconque congru à *a* modulo *n*.

Les entiers relatifs congrus à *a* modulo *n* sont les entiers de la forme $b+kn$ $(k \in \mathbb{Z})$.

4°) Cas particulier

Les entiers congrus à 0 modulo *n* sont les multiples de *n*.

5°) Utilisation pratique : tableaux de congruences

Il s'agit d'une méthode très utile en pratique.
On utilise les propriétés opératoires des congruences (additions, multiplication, puissances).

III. Propriétés immédiates de la relation de congruence

1°) Propriété 1 (réflexivité)

$a \equiv a \pmod{n}$

2°) Propriété 2 (symétrie)

Si $a \equiv b \pmod{n}$, alors $b \equiv a \pmod{n}$.

3°) Propriété 3 (transitivité)

Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$.

IV. Congruences et opérations

a, b, c, d sont des entiers relatifs.
k est un entier naturel.

1°) Propriété 1 (addition ou soustraction d'un même nombre)

Si $a \equiv b \pmod{n}$, alors $a+c \equiv b+c \pmod{n}$
et $a-c \equiv b-c \pmod{n}$.

2°) Propriété 2 (addition ou soustraction membre à membre)

Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a+c \equiv b+d \pmod{n}$
et $a-c \equiv b-d \pmod{n}$.

3°) Propriété 3 (produit par un même entier)

Si $a \equiv b \pmod{n}$, alors $a \times c \equiv b \times c \pmod{n}$.

4°) Propriété 4 (produit membre à membre)

Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a \times c \equiv b \times d \pmod{n}$.

5°) Propriété 5 (élévation des deux membres à un même exposant entier naturel)

Si $a \equiv b \pmod{n}$, alors $a^k \equiv b^k \pmod{n}$.

V. Congruences et division euclidienne (1)

1°) Propriété fondamentale

Tout entier relatif a est congru modulo n à son reste dans la division euclidienne par n.

2°) Un corollaire important

Tout entier relatif a est soit congru à 0 mod. n, soit congru à 1 mod. n … soit congru à $n-1$ mod. n.

3°) Cas particuliers

• Congruence modulo 2

Tout entier relatif est soit congru à 0 modulo 2 soit congru à 1 modulo 2.

Il est important de retenir les équivalences suivantes pour n entier relatif quelconque.

n est pair $\Leftrightarrow n \equiv 0 \pmod 2$.
n est impair $\Leftrightarrow n \equiv 1 \pmod 2$.

• Congruence modulo 3

Tout entier relatif est soit congru à 0 mod. 3 soit congru à 1 mod. 3, soit congru à 2 mod. 3.

VI. Congruences et division euclidienne (2)

1°) Propriété

a et b sont deux entiers relatifs.
$a \equiv b \pmod n$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

2°) Conséquence

a est un entier relatif.
$a \equiv r \pmod n$ et $0 \leqslant r < n \Leftrightarrow r$ est le reste de la division euclidienne de a par n.

► Application aux calculs de restes de divisions euclidiennes d'entiers

VII. Résultats sur les congruences modulo 3 et modulo 9

Tous les résultats énoncés pour les congruences modulo 9 sont valables pour les congruences modulo 3.

1°) Résultat préliminaire sur les puissances de 10

$\forall k \in \mathbb{N} \quad 10^k \equiv 1 \pmod 9$

2°) Propriété

Tout entier naturel N est congru à la somme de ses chiffres en base 10 modulo 9.

N ≡ somme des chiffres de N en base dix (mod. 9)

La démonstration est évidente à partir de la décomposition en base 10 de N.

On pose $N = \overline{a_n a_{n-1} ... a_0}$ où a_0, a_1, … a_n sont des entiers naturels inférieurs ou égaux à 9 (et $a_n \neq 0$).

On écrit la décomposition en base 10 de N : $N = a_n \times 10^n + a_{n-1} \times 10^{n-1} + ... + a_1 \times 10 + a_0$.
Le résultat découle de la petite propriété donnée au **1°)** : toute puissance de 10 d'exposant entier naturel est congrue à 1 modulo 9.

3°) Applications

Cette propriété permet de justifier :
- la méthode de calcul du reste de la division euclidienne d'un entier naturel par 3 ou par 9 à la main ;
- les critères de divisibilité d'un entier naturel par 3 et par 9 ;
- la méthode de la preuve par 9 pour la multiplication.

VIII. Résultats sur les congruences modulo 10, 100, 1000 etc.

Propriété :

- Tout entier naturel est congru modulo 10 au chiffre des unités de son écriture en base 10.

- Tout entier naturel est congru modulo 100 au nombre formé par les deux derniers chiffres de son écriture en base 10.

- Tout entier naturel est congru modulo 1000 au nombre formé par les deux derniers chiffres de son écriture en base 10.

Démonstration :

On utilise la décomposition en base 10 d'un entier naturel.

VIII. Quelques méthodes importantes

1°) Calculer le reste d'une division euclidienne d'un entier relatif A par un entier naturel $n \geqslant 2$.

► On raisonne en congruence modulo *n*. On utilise les propriétés opératoires des congruences (additions, multiplications, puissances).

2°) Démontrer qu'un entier A est divisible par un entier naturel $n \geqslant 2$.

► On raisonne en congruence modulo *n*. On démontre que $A \equiv 0 \pmod{n}$.
On peut être amené à utiliser le petit résultat suivant qui est très facile à démontrer.

> *a* et *b* sont deux entiers relatifs tels que $a \equiv b \pmod{n}$.
> *a* divisible par $n \Leftrightarrow$ *b* divisible par *n*.

3°) Résoudre une équation donnée par une congruence.

► On utilise un tableau de congruence (possible quand on raisonne en congruence modulo n pour de petites valeurs de n).

Exemple : Déterminer les entiers relatifs x tels que $5x \equiv 3 \pmod 8$.

4°) Établir une propriété valable pour tout entier relatif.

► On utilise un tableau de congruence (possible quand on raisonne en congruence modulo n pour de petites valeurs de n).

Exemple : Démontrer que pour tout entier relatif x le nombre $x^3 - x$ est divisible par 3.
On raisonne en congruence modulo 3.

4°) Logique et congruences

On peut ajouter ou soustraire un même entier relatif aux deux membres d'une relation de congruence.
On obtient une nouvelle relation de congruence qui est équivalente.

Autrement dit, on a les équivalences suivantes pour a, b, c entiers relatifs :
$a \equiv b \pmod n \Leftrightarrow a + c \equiv b + c \pmod n$
$a \equiv b \pmod n \Leftrightarrow a - c \equiv b - c \pmod n$

En revanche, les propriétés pour le produit et les puissances ne fonctionnent que dans un sens :

$a \equiv b \pmod n \Rightarrow a \times c \equiv b \times c \pmod n$; $a \equiv b \pmod n \Rightarrow a^k \equiv b^k \pmod n$.

Il n'y a pas équivalence.

Il faut faire très attention à ne pas écrire trop vite des équivalences.

Exemple :

$2^2 \equiv 1^2 \pmod 3$ mais 2 n'est pas congru à 1 modulo 3 !

Un cas cependant d'équivalence vraie pour le produit : $a \equiv b \pmod n \Leftrightarrow -a \equiv -b \pmod n$.

5°) Une technique importante : passer d'une égalité à une congruence

Exemples :

① On suppose que x et y sont deux entiers relatifs vérifiant l'égalité $5x - 3y = 1$.

On peut alors écrire : : $5x \equiv 1 \pmod 3$.

On peut également écrire : $-3y \equiv 1 \pmod 5$.

② On suppose que x et y sont deux entiers relatifs vérifiant l'égalité $17x-3y=1$.

On peut alors écrire : : $17x \equiv 1 \pmod 3$ et même $2x \equiv 1 \pmod 3$ car $17 \equiv 2 \pmod 3$.

Dans une égalité modulo n, on peut remplacer un nombre par un nombre qui lui est congru modulo n.