Chapitre 5 — Congruences dans $\mathbb{Z}$

I- Généralités

Définition

Soit $n \in \mathbb{N}^*$ et a et b deux entiers relatifs.

Dire que <u>a et b sont congrus modulo n</u> lorsque a et b ont le même reste dans la division euclidienne par n.

On adopte la notation suivante : $a \equiv b\ [n]$ que l'on lit : « a est congru à b modulo n », on note aussi $a \equiv b\ (n)$ ou encore $a \equiv b \mod n$.

Attention au symbole de congruence $\equiv$: *il n'a rien à voir avec le signe = usuel* !!!

Exemples

15 et 22 sont congrus modulo 7.

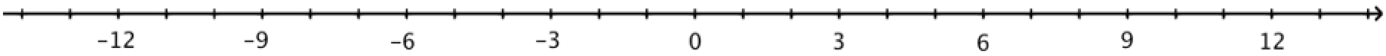
Citer deux entiers congrus modulos 4.

Expliquer pourquoi $212 \equiv 335\ [3]$.

Remarque : De-par la définition, $a \equiv b\ [n]$ revient à dire que $b \equiv a\ [n]$. On dit que la relation de congruence modulo n est symétrique.

Exemple bis

Sur la droite graduée ci-dessous, on a représenté quelques multiples de 3 (points avec abscisse chiffrée) :



Construire au stylo verts les entiers de cette droite congrus à 1 modulo 3, et en rouge les entiers congrus à 2 modulo 3.

Nous allons voir une propriété importante qui rend plus " maniable " la notion d'entiers congrus modulo n.

Propriété

Soit $n \in \mathbb{N}^*$ et a et b deux entiers relatifs.

$a \equiv b\ [n]$ si et seulement si on a : <u>n divise $a-b$</u> ou encore <u>$a-b$ est un multiple de n</u>.

Ainsi, $a \equiv b\ [n]$ si et seulement si il existe un entier $\boldsymbol{k}$ tel que : ....

Preuve :

✂--

Exemples

Est-il vrai que $2026 \equiv 8\ [10]$?

Donner l'expression générale des nombres congrus à 4 modulo 11.

♥♥ x est un entier. Que signifie le fait que : $x \equiv 0\ [2]$? Que signifie que $x \equiv 1\ [2]$? ♥♥

✂--

Propriétés triviales de la relation de congruence

Soit $n \in \mathbb{N}^*$.

- Pour tout entier relatif a, $a \equiv a\ [n]$.

♥♥- $a \equiv 0\ [n]$ si et seulement si ....♥♥

- Pour tout entier relatif a, $a \equiv r\ [n]$, où r désigne le reste dans la division euclidienne de a par n.

- ***Transitivité de la relation de congruence :***

Pour tous entiers a, b et c, si $a \equiv b\ [n]$ et si $b \equiv c\ [n]$, alors ....

Preuve :

✂---

Exemples

$31 \equiv 4\ [27]$ et $4 \equiv 301\ [27]$, donc $301 \equiv 31\ [27]$.

Exercice 1

1) Déterminer si l'affirmation suivante est vraie ou fausse, en justifiant :

Si $a \equiv b\,[n]$, alors le reste dans la division euclidienne de a par n est b.

2) A quoi est congru modulo 10 tout entier naturel ?

Exemple : $2026 \equiv \cdots [10]$.

✂---

Nous allons voir à présent des propriétés et l'utilité et l'efficacité des congruences.

♥♥ ***Propriétés de compatibilité de la relation de congruence avec les opérations usuelles*** ♥♥

Soient a, b, c et d des entiers relatifs, et n un entier naturel non nul.

i) ♥♥ Si $a \equiv b\ [n]$ et si $c \equiv d\ [n]$, alors ....♥♥ : On dit que la relation de congruence est compatible avec l'addition.

Remarque : on a aussi : ♥♥ ....♥♥, donc la relation de congruence est compatible avec la soustraction, ce qui n'a rien de surprenant, vu que toute soustraction n'est autre qu'une addition particulière.

ii) ♥♥ Si $a \equiv b\ [n]$ et si $c \equiv d\ [n]$, alors ....♥♥ : On dit que la relation de congruence est compatible avec la multiplication.

iii) ♥♥ Pour tout entier naturel k non nul, si $a \equiv b\ [n]$ alors.................................♥♥ : On dira que la relation de congruence est compatible avec les puissances.

Preuve :

✂---

Remarque : attention, la réciproque de chacune des affirmations suivantes est fausse ! Vous devez vous en convaincre à l'aide de contrexemples faciles à fabriquer.

De i), on déduit que **si $a \equiv b$ [n], alors, pour tout entier relatif c, $a+c \equiv b+c$ [n].** Pourquoi ?

De ii), on déduit que **si $a \equiv b$ [n], alors, pour tout entier relatif c, $ac \equiv bc$ [n].** Pourquoi ?

Attention, même si ces règles sont similaires à celles sur les égalités, rappelons que la relation de congruence et l'égalité sont deux notions bien distinctes !

Si $ac \equiv bc$ [n], il est en général faux de dire que $a \equiv b$ [n], c'est-à-dire qu'on on ne simplifie pas par c (même si c est non nul) une congruence ! Encore un point qui diffère par rapport aux égalités.

Exemple : $6\times 3 \equiv 6\times 1$ [12], *mais* 3 *n'est pas congru à* 1 *modulo* 12 !

Application phare des congruences : preuve des critères de divisibilités usuels du système décimal.

Définition

Soit N un entier naturel. Notons $a_0, a_1, \dots\dots, a_n$ les chiffres respectifs des unités, dizaines, centaines…..de son écriture décimale. [$a_0, \dots\dots, a_n$ sont donc des entiers compris entre 0 et 9].

On a donc : $N = a_0 \times 10^0 + a_1\times 10^1 + a_2\times 10^2 + \dots\dots + a_n\times 10^n = \sum_{k=0}^{n} a_k \times 10^k$.

On notera parfois : $N = \overline{a_n a_{n-1} \dots\dots a_1 a_0}$ (La barre est pour éviter la confusion avec l'écriture du produit des chiffres constituant N dans l'écriture d'un entier en base 10).

Par exemple : soit $N = 213$. On a : $N = 2\times 10^2 + 1\times 10^1 + 3\times 10^0$.

Décomposer de la même façon : 3258 :

♥ ♥ ***Critères de divisibilité usuels du système décimal*** ♥ ♥

- ✓ *Un entier naturel N est divisible par 2 (N est pair) si et seulement si son chiffre des unités est lui-même pair.*

- ✓ *Un entier naturel N est divisible par 5 si et seulement si son chiffre des unités vaut 0 ou 5.*

- ✓ *Un entier N est divisible par 3 si et seulement si la somme des chiffres de N est un multiple de 3.*

- ✓ *Un entier est divisible par 9 si et seulement si la somme des chiffres de N est un multiple de 9.*

- ✓ *Un entier N est divisible par 11 si et seulement si, avec les notations de la définition,* $\sum_{k=0}^{n} (-1)^k \times a_k$ est un multiple de 11, ce qui revient à dire que la somme des chiffres de N de rang pair à laquelle on soustrait la somme des chiffres de N de rang impair est un multiple de 11.

Preuve :

✂---

Exemple

Etablir que 201520142013 n'est pas un multiple de 11, puis que $A = 201520142013^{2016} - 4018^{2016}$ est un multiple de 11.

Pour votre culture, il existe des critères de divisibilité par k, pour tout entier $k > 1$. Cependant, ils sont peu pratiques d'utilisation, voilà pourquoi on ne vous demande pas de les retenir.

II-Farandole d'applications des congruences à la résolution de problèmes divers et variés.

Exercice 0

1) Quelle heure sera-t-il 213 heures après 14 heures ?
2) Quand on joue à la belote par exemple, au bout de quelques manches, on ne sait en général plus à qui revient la charge de distribuer les cartes….

Matt, Maeva, Matthieu et Mathilde distribuent à tour de rôle, dans cet ordre, les cartes.

Matt a commencé à donner les cartes lors la première manche. Qui devra distribuer les cartes à la 327*ième* manche (en supposant que les joueurs aient une très forte addiction au jeu de belote) ?

✂---

Exercice 1

a) Donner le chiffre auquel est congru, modulo 10, chacun des entiers suivants :
2026 ; 2026^2 ; 2026^3 ; 2026^4. Pour les puissances suivantes 2026^5 ; 2026^6 …. que peut-on prévoir ?

b) En déduire quel est le chiffre des unités de l'entier 2026^{2027}.

✂---

Exercice 2

1) A l'aide d'un tableau de congruences, montrer que le produit de trois entiers consécutifs est un multiple de 3.
2) Soit n un entier naturel. Démontrer que si n n'est pas divisible par 5, alors $(n^2-1)(n^2-4)$ est divisible par 5.

✂---

Exercice 3

n est un entier naturel. Conjecturer une propriété commune aux entiers de la forme : $3 \times 2^{4n+2} - 7$.
Prouver que cette dernière est vraie pour tout entier naturel n.

✂---

Exercice 4

Démontrer que pour tout entier naturel n, $3^{2n+1} + 2^{n+2}$ est divisible par 7.

✂---

Exercice 5

1) En utilisant un tableau de congruences, établir que le carré d'un entier naturel est congru à 0, 1 ou 4 *modulo* 8.

2) Soit n un entier naturel tel que $n \equiv 7$ [8]. Etablir que n ne peut pas être la somme de trois carrés d'entiers.

✂---

Exercice 6

a) Soit n un entier. Déterminer les deux chiffres, les plus petits possibles, auxquels n^2 est congru modulo 4.

b) Dans le plan muni d'un repère orthonormé d'origine O, on considère le cercle $\mathscr{C}$ de centre O et de rayon $5\sqrt{7}$. Existe-t-il des points à coordonnées entières situés sur le cercle $\mathscr{C}$?

Exercice 7

1) Déterminer tous les entiers x tels que : $x - 1 \equiv 11$ [5].
2) Prouver l'équivalence suivante : $3x \equiv 4$ [7] $\Leftrightarrow x \equiv 6$ [7].

✂--

Exercice sublime

Soit N un entier écrit en base 10. On appelle $p(N)$ un permuté de N, c'est-à-dire un nombre entier écrit avec les mêmes chiffres que ceux de N, écrits dans un ordre arbitraire.

Démontrer que pour tout entier N, $N - p(N)$ est un multiple de 9.

✂--

Exercice 8 (DM ?)

(u_n) est la suite définie par : $u_0 = 1$ et pour tout entier naturel n, $u_{n+1} = 10u_n + 21$.

1) Calculer u_1, u_2 et u_3.

2)
a) En raisonnant par récurrence, démontrer que pour tout entier naturel n, $3u_n = 10^{n+1} - 7$.

b) En déduire que pour tout entier naturel n, u_n n'est divisible ni par 2, ni par 3 ni par 5, ni par 11.