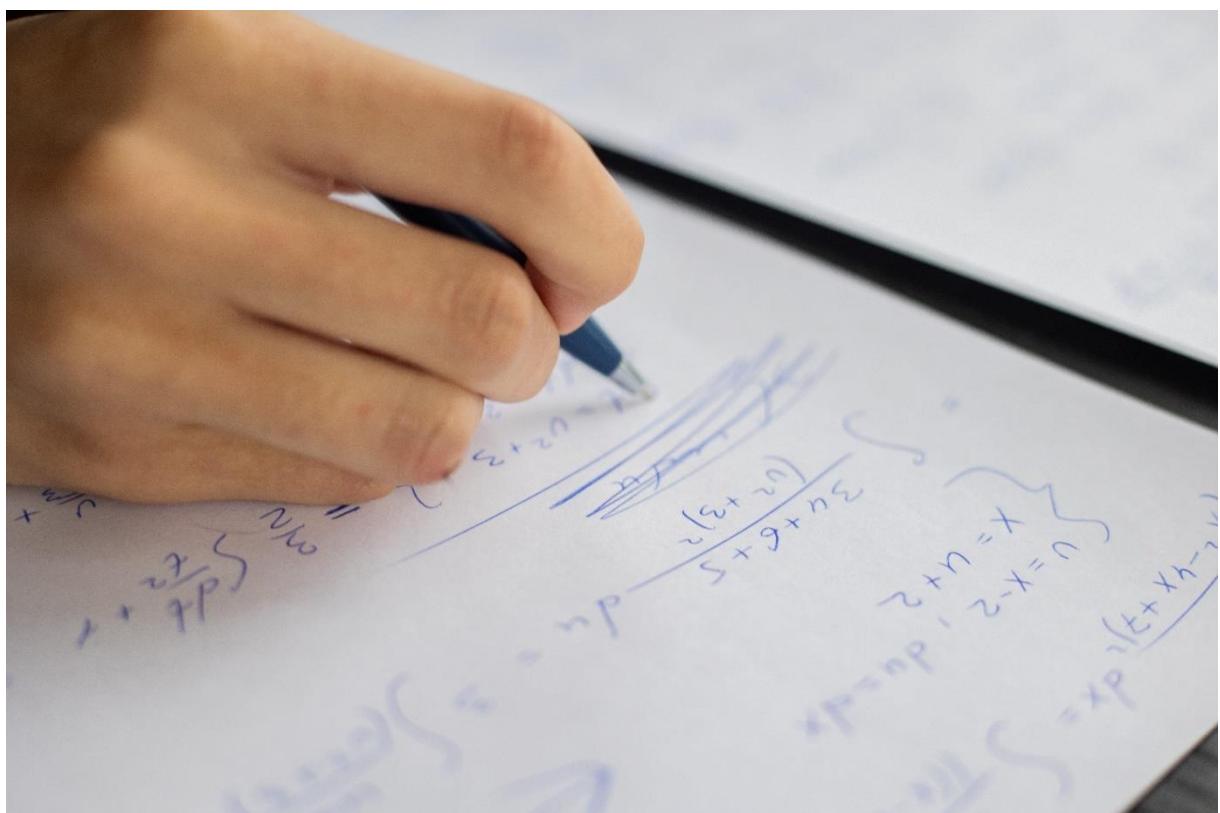


ARITHMETIQUE

4. Congruences

- Cours



Elliot LOUVEAU

elliot.louveau@eduservices.org

TABLE DES MATIERES

DEFINITIONS	2
En français :	2
En mathématiques :.....	2
Qu'est-ce que deux nombres congrus ?	2
Exemples	3
PROPRIETES.....	5
Congrus si différence multiple de n	5
Démonstration	5
Exemples	6
Transitivité !.....	7
Exemples :	7
Congruence et opérations arithmétiques (1).....	8
Congruence et opérations arithmétiques (2).....	9
Rappel sur les règles avec les puissances.....	9
À QUOI ÇA SERT ?	10
Déterminer si une formule est multiple d'un nombre	10
Trouver le reste d'une division euclidienne complexe.....	11
Établir des protocoles de chiffrements	12
INVERSE MODULAIRE.....	13

/ **13**

RESOLUTION D'EQUATIONS MODULAIRE 13

L'inverse :	13
L'inverse modulaire :.....	14
Résolution d'équation modulaire	15

DEFINITIONS

EN FRANÇAIS :

D'après Larousse : *Fait de coïncider, de s'ajuster parfaitement.*

EN MATHEMATIQUES :

D'après le CNRTL (Centre National de Ressources Textuelles et Lexicales) :
Relation qui existe entre deux nombres congrus.

Qu'est-ce que deux nombres congrus ?

Soit n un entier naturel ≥ 2 . On dit que deux entiers naturels a et b sont **congrus modulo n** (ou que a est congrus à b modulo n) si et seulement si a et b ont le même reste dans la division euclidienne par n .

Cette relation se note $a \equiv b[n]$ ou $b \equiv a[n]$

Autrement dit :

En faisant la division euclidienne de a par n on obtient un reste. Si en faisant la division euclidienne de b par n on obtient le même reste, on dit que a et b sont congrus modulo n .

Exemples

1) 34 et 29 sont-ils congrus modulo 5 ?

Oui, car $34 = 6 \cdot 5 + 4$ et $29 = 5 \cdot 5 + 4$; ils ont le même reste dans la division euclidienne par 5. On note $34 \equiv 29[5]$

2) 67 est-il congru à 139 modulo 12 ?

$$67 = 12 \cdot 5 + 7 \text{ et } 139 = 12 \cdot 11 + 7$$

Donc $67 \equiv 139[12]$

3) 90 et 80 sont-ils congrus modulo 11 ?

90 et 80 ne sont pas congrus modulo 11, car les restes dans les divisions Euclidiennes. $90 = 8 \cdot 11 + 2$; $80 = 7 \cdot 11 + 3$

⚠️ À noter :

- Quelques soit un nombre entier a , $a \equiv a[n]$ **et** $a \equiv r[n]$, r étant le reste de la division euclidienne de a par n .

Exemples :

$$5 \equiv 1[2] \text{ car } 5 = 2 \cdot 2 + 1$$

$$123 \equiv 2[11] \text{ car } 123 = 11 \cdot 11 + 2$$

- Un nombre entier a est divisible par n si et seulement si $a \equiv 0[n]$

Exemples :

$$30 \text{ est divisible par } 6 \text{ car } 30 = 6 \cdot 5 + 0 \Leftrightarrow 30 \equiv 0[6]$$

3

-- Exercices : Les bases de la congruence

PROPRIETES

CONGRUS SI DIFFERENCE MULTIPLE DE N

Soient a et b deux entiers naturels tels que $a > b$ et soit n un entier naturel non nul. a est congru à b modulo n si et seulement si $a - b$ est multiple de n .

Rappel :

Dire que $a - b$ est multiple de n revient à dire que $a - b = n * k$ avec $k \in \mathbb{Z}^1$.

Démonstration

Si $a \equiv b[n]$, alors a et b ont le même reste dans la division euclidienne par n

Donc on a $a = nq + r$ et $b = nq' + r$ donc :

$$a - b = (nq + r) - (nq' + r) = nq + r - nq' - r = nq - nq' = n(q - q')$$

q et q' sont deux entiers donc $q - q'$ est un entier $\Rightarrow a - b$ est multiple de n .

¹ \mathbb{Z} = Ensemble des entiers relatifs : nombre sans décimal, positif ou négatif

Exemple

101 et 66 sont-ils congrus modulo 7 ?

Pour répondre à cette question soit

- *on regarde si le reste de la division euclidienne de 101 et de 66 par 7 est le même*
- ***on regarde si la différence est multiple de 7***

$$101 - 66 = 35 ; 35 \text{ est multiple de } 7 \text{ car } 35 = 5 * 7$$

D'après la propriété, on peut affirmer que $101 \equiv 66[7]$

⚠️ Extrapolation

On peut déduire d'autres congruences à partir de celle-ci :

$$101 \equiv 66[7], \text{ ajoutons une fois 7 à 66. } 66 + 7 = 73.$$

66 et 73 ont logiquement le même reste dans la division euclidienne par 7.
 $66 = 7 * 9 + 3$ et $73 = 7 * 10 + 3$; peu importe combien de fois j'ajoute ou je retire 7, le nombre obtenu par rapport à mon nombre de départ aura toujours le même reste dans la division euclidienne par 7.

Si a et b ont le même reste dans la division euclidienne par n alors $a \equiv b[n] \Leftrightarrow a \equiv b + n[n] \Leftrightarrow a \equiv b + 2n[n] \Leftrightarrow a \equiv b \pm k * n[n]$ avec $k \in \mathbb{Z}$.

⇒ ***Je peux ajouter ou retirer autant de fois n à b que je veux, je garderai la congruence. Idem avec a .***

$$101 \equiv 66[7] \text{ alors } 101 \equiv 59[7] \text{ et aussi } 101 \equiv 52[7] \text{ et encore } 94 \equiv 73[7] \dots$$

⇒ *en ajoutant ou retirant 7 à chaque fois on garde le fait que les deux nombres ont le même reste dans la division euclidienne par 7 et que $a - b$ est multiple de 7.*

Pour simplifier l'écriture d'une congruence, on l'écrira de telle sorte à ce que b soit compris entre 0 et n .

$$101 \equiv 66[7] \Leftrightarrow 101 \equiv 3[7] \text{ car } 101 = 7 * 14 + 3$$

TRANSITIVITE² !

Si $a \equiv b[n]$ et que $b \equiv c[n]$ alors $a \equiv c[n]$

Exemples :

1) $139 \equiv 67[12] ; 67 \equiv 7[12]$ *Donc* $139 \equiv 7[12]$

Cette propriété permet d'écrire des chaînes d'égalité sans ambiguïté et de remplacer une valeur par une autre :

$$139 \equiv 67 \equiv 7[12]$$

2) Soit $N = 2^2 * 3 * 7 * 19$, Déterminez le reste de la division euclidienne de N par 8.

⇒ Chercher le reste de la division euclidienne de N par 8 revient à chercher le plus petit entier positif auquel N est congru modulo 8.

La technique est la suivante : on effectue petit-à-petit les multiplications, et dès qu'on dépasse 8, on réduit modulo 8 :

$$N \equiv 12 * 7 * 19 \equiv 4 * 7 * 3 \equiv 28 * 3 \equiv 4 * 3 \equiv 12 \equiv 4[8]$$

Comme $0 \leq 4 < 8$, 4 est le reste de la division euclidienne de N par 8.

² Définition transitivité : « Propriété d'une relation binaire dont la suite de chiffres liés consécutivement se termine par une relation entre le premier et le dernier. Exemple : Si $X=Y$ et $Y=Z$ alors $X=Z$, il s'agit d'une transitivité.»

Source : <https://www.linternaute.fr/dictionnaire/fr/definition/transitivite/>

Exercices

CONGRUENCE ET OPERATIONS ARITHMETIQUES (1)

Soient a, b et p des entiers naturels en n un entier naturel non nul.

Si $a \equiv b[n]$ alors :

- $a + p \equiv b + p[n]$
 - $20 \equiv 16 [4] \Leftrightarrow 20 + 3 \equiv 16 + 3[4] \Leftrightarrow 23 \equiv 19[4]$
- $a - p \equiv b - p[n]$
 - $20 \equiv 16 [4] \Leftrightarrow 20 - 7 \equiv 16 - 7[4] \Leftrightarrow 13 \equiv 9[4]$
- $pa \equiv pb[n]$
 - $20 \equiv 16 [4] \Leftrightarrow 20 * 3 \equiv 16 * 3[4] \Leftrightarrow 60 \equiv 48[4]$

\triangleleft On ne peut pas simplifier une congruence avec la division comme une égalité classique : **$2a \equiv 2b[n]$ n'implique pas $a \equiv b[n]$.**

$20 \equiv 16 [4]$ mais 10 et 8 ne sont pas congrus modulo 4.

- $a^p \equiv b^p[n]$
 - $9 \equiv 5 [4] \Leftrightarrow 9^2 \equiv 5^2[4] \Leftrightarrow 81 \equiv 25[4]$

\triangleleft On peut éléver à la puissance mais pas réduire.

- $6^2 \equiv 36 \equiv 0[4]$ par contre $6 \equiv 2[4]$

CONGRUENCE ET OPERATIONS ARITHMETIQUES (2)

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

Si $a \equiv b[n]$ et $c \equiv d[n]$ alors :

- $a + c \equiv b + d[n]$ et $a - c \equiv b - d[n]$
 - $2023 \equiv 1[3]$ et $1000 \equiv 1[3]$
 - $2023 + 1000 \equiv 3023 \equiv 1 + 1 \equiv 2[3]$
 - $2023 - 1000 \equiv 1023 \equiv 1 - 1 \equiv 0[3]$
- $ac \equiv bd[n]$
 - $1000 * 2023 \equiv 1 * 1 \equiv 1[3]$ c'est-à-dire $2014\,000 \equiv 1[3]$

--- Exercices : Congruences et opérations arithmétiques ;

RAPPEL SUR LES REGLES AVEC LES PUISSANCES

$$x^3 = x * x * x = x^2 * x ;$$

$$x^5 = x^3 * x^2 ;$$

$$x^{12} = x^6 * x^6 = (x^6)^2 ;$$

$$x^{13} = (x^3)^4 * x ;$$

$$x^{1150} = (x^2)^{575} = (x^5)^{230} \dots ;$$

$$1^{3210} = 1$$

$$(-1)^{\text{nb paire}} = 1$$

$$(-1)^{\text{nb impair}} = -1$$

À QUOI ÇA SERT ?

DETERMINER SI UNE FORMULE EST MULTIPLE D'UN NOMBRE

- *Un nombre a est multiple d'un nombre b si $a = kb + 0$, $k \in \mathbb{Z}$*
- *Le reste de la division euclidienne de a par b est nul*
 $\Rightarrow a \equiv 0[b]$

Pour démontrer qu'une formule / une opération intégrant une inconnue est multiple d'un nombre, nous allons utiliser un tableau de congruence.

Exemple : Démontrer que $n^5 + 4n$ est multiple de 5

\Rightarrow Revient à démontrer que pour tout n le reste de la division euclidienne de $n^5 + 4n$ est toujours égale à 0, autrement dit, démontrer que pour tout n , $n^5 + 4n \equiv 0[5]$

On sait que dans la division euclidienne par 5, les restes possibles sont 0, 1, 2, 3 et 4.

Pour faire la démonstration il suffit de faire un tableau de congruence en étudiant à quoi congru $n^5 + 4n$ dans tous les cas possibles :

On décompose $n^5 + 4n$ de sorte à se faciliter les calculs :

- $n^5 = n^2 * n^3$, donc je calcule d'abord n^2 en ramenant la congruence à un nombre entre 0 et 4, puis n^3 en calculant $n^2 * n$ et en ramenant le résultat à un nombre entre 0 et 4.
- $4n$ puis la somme $n^5 + 4n$ en ramenant le résultat à un nombre entre 0 et 4

$n \equiv \dots [5]$	0	1	2	3	4
$n^2 \equiv \dots [5]$	0	1	4	4	1
$n^3 \equiv \dots [5]$	0	1	3	2	4
$n^5 \equiv \dots [5]$	0	1	2	3	4
$4n \equiv \dots [5]$	0	4	3	2	1
$n^5 + 4n \equiv \dots [5]$	0	0	0	0	0

Dans tous les cas $n^5 + 4n \equiv 0[5]$, donc $n^5 + 4n$ est un multiple de 5

TROUVER LE RESTE D'UNE DIVISION EUCLIDIENNE COMPLEXE

Exemple : Déterminer le reste de la division euclidienne de $6^{28} * 3^{1234}$ par 7

La technique consiste d'abord à déterminer indépendamment à quoi est congru 6^{28} modulo 7 et 3^{1234} modulo 7 puis de faire la multiplication.

Pour ça nous allons utiliser la propriété qui dit que si $a \equiv b[n]$ alors $a^p \equiv b^p[n]$

Nous allons également essayer de simplifier les calculs en cherchant si possible une congruence qui nous permettra de décomposer notre puissance facilement. Trouver une puissance qui est congru à 1 ou -1 nous aidera beaucoup par exemple.

$$6 \equiv 6 \equiv -1[7]$$

$$6^{28} \equiv -1^{28} \equiv 1$$

$$3^2 \equiv 9 \equiv 2[7]$$

$$3^3 \equiv 3^2 * 3 \equiv 2 * 3 \equiv 6 \equiv -1[7]$$

$$1234 = 3 * 411 + 1$$

$$3^{1234} \equiv 3^{3*411+1} \equiv (3^3)^{411} * 3 \equiv (-1)^{411} * 3 \equiv -1 * 3 \equiv -3 \equiv 4[7]$$

$$6^{28} * 3^{1234} \equiv 1 * 4 \equiv 4[7]$$

\Rightarrow Le reste de la division euclidienne de $6^{28} * 3^{1234}$ par 7 est donc de 4.

ÉTABLIR DES PROTOCOLES DE CHIFFREMENTS

Voir TD : chiffrement affine ci-après.

INVERSE MODULAIRE / RESOLUTION D'EQUATIONS MODULAIRES

L'INVERSE :

En mathématique on dit que deux nombres a et b sont inverses si $a * b = 1$

Exemple : $\frac{1}{4}$ est l'inverse de 4 car $\frac{1}{4} * 4 = 1$

On utilise l'inverse pour résoudre des équations. Par exemple lorsque l'on cherche à résoudre $4x = 32$ on va diviser par 4 des deux cotés de l'équation pour trouver $x = \frac{32}{4} = 8$.

« Diviser c'est multiplier par son inverse »

Quand on divise par 4 dans l'équation précédente, on multiplie en fait des deux côtés par $\frac{1}{4}$; qui est l'inverse de 4

L'INVERSE MODULAIRE :

En arithmétique modulaire l'inverse d'un nombre a modulo n est un nombre b tel que $a * b \equiv 1[n]$

⚠ Pour qu'un nombre a soit inversable modulo n ; il faut que a et n soient premiers entre eux.

⚠ Étant donné que nous sommes modulo n , un nombre peut avoir plusieurs inverses en ajoutant ou retirant $k*n$ avec $k \in \mathbb{Z}$.

Exemples :

a) Modulo 5, donner un inverse du chiffre 3 :

Je cherche un nombre x tel que $3x \equiv 1[5]$

À l'aide d'un tableau de congruence :

Je sais qu'un nombre x modulo 5 sera congru soit à 0, 1, 2, 3 ou 4

$x \equiv \dots [5]$	0	1	2	3	4
$3x \equiv \dots [5]$	0	3	1		

$3*2$ congru à 1 modulo 5 ; 2 est donc un inverse de 3 modulo 5, pas besoin de calculer le reste

b) Modulo 7, donner un inverse du chiffre 5 :

Je cherche un nombre x tel que $5x \equiv 1[7] \dots$

Autrement dit, je cherche un nombre dans la table de 5 qui soit supérieur à 1 d'un nombre dans la table de 7...

$$5 * 3 \equiv 2 * 7 + 1 \equiv 1[7]$$

3 est donc l'inverse de 5 modulo 7

c) Modulo 22, donner un inverse du chiffre 7 :

Je cherche un nombre x tel que $7x \equiv 1[22]$

Indice : Si je trouve un nombre x tel que $7x \equiv -1[22]$ je pourrais en déduire qu'un inverse de 7 modulo 22 sera $-x$.

$$\text{⚠ } a * x \equiv -1[n] \Leftrightarrow a * (-x) \equiv 1[n]$$

$$7 * 3 = 21 \text{ Donc } 7 * 3 \equiv 21 \equiv -1[22]$$

$$7 * (-3) \equiv -21 \equiv 1[22]$$

-3 est donc un inverse de 7 modulo 22

$$-3 + 22 = 19 \text{ l'est aussi pour rappel } 7 * 19 \equiv 133 \equiv 1[22]$$

Tous les nombres entiers congrus à -3 modulo 22 seront des inverses de 7 modulo 22.

RESOLUTION D'EQUATION MODULAIRE

Trouver un inverse modulaire va nous permettre de résoudre des équations avec des congruences. Dans notre exemple précédent nous avons trouvé qu'un inverse de 7 modulo 22 était -3.

Si je cherche à résoudre l'équation $7x \equiv 5[22]$:

Dans le cadre d'une égalité on multiplierait par $\frac{1}{7}$ pour « annuler » le 7 devant le x. Ici dans une équation avec une congruence, on va multiplier

par l'inverse de 7 modulo 22. Nous avons déterminé précédemment qu'un inverse de 7 modulo 22 était -3.

$$7x \equiv 5[22]$$

$$\text{Donc } 7x * (-3) \equiv 5 * (-3)[22]$$

$$\text{Donc } -21x \equiv -15[22]$$

$$\text{Donc } x \equiv -15 \equiv 7[22]$$

⚠ Comme on ne peut pas diviser avec les congruences, on ne peut pas mettre de signe d'équivalence entre deux lignes lorsque l'on multiplie dans une équation avec des congruences. Pour bien faire il faudra toujours vérifier la réciproque pour conclure sur la solution.

Réciproquement :

$$x \equiv 7[22]$$

$$7x \equiv 7 * 7 \equiv 49 \equiv 27 \equiv 5 [22]$$

$$S = \{ 7 + 22k, k \in \mathbb{Z} \}$$

Pour info : [S = « Solution »]

— Exercices : Inverses et équations avec des congruences

