CONGRUENCES

I Définition et propriétés

Soit m un entier naturel non nul. Dire que deux entiers a et b sont congrus modulo m signifie qu'ils ont le même reste dans la division euclidienne par m.

On note $a \equiv b \ [m]$ et on lit « a est congru à b modulo m ».

Ex : $28 \equiv 13 \ [3]$. En effet, $28 = 3 \times 9 + 1$ et $13 = 3 \times 4 + 1$

$-13 \equiv 27 \ [5]$. En effet, $-13 = 5 \times (-3) + 2$ et $27 = 5 \times 5 + 2$

Important : Si r est le reste de la division de a par m alors $a \equiv r \ [m]$: on se servira très souvent de cette égalité, laquelle est « la plus simple »

Si on reprend les exemples précédents, $28 \equiv 13 \ [3]$ mais également $28 \equiv 1 \ [3]$ car $28 = 3 \times 9 + 1$.

Et $-13 \equiv 27 \ [5]$ mais également $-13 \equiv 2 \ [5]$ car $-13 = 5 \times (-3) + 2$

Remarque : $a \equiv 0 \ [m]$ si et seulement si m divise a

Théorème : Soit m un entier naturel non nul. Pour tous entiers relatifs a et b, on a :

$$a \equiv b \ [m] \iff m|(a-b)$$

Conséquence : $a \equiv b \ [m] \iff a = b + km$

Preuve : ($\Rightarrow$) Supposons que $a \equiv b \ [m]$.

On a donc $a = mq + r$ et $b = mq' + r$

D'où $a - b = m(q - q')$ donc $m|(a-b)$

($\Leftarrow$) Réciproquement, supposons que $m|(a-b)$.

On a alors $a - b = mk$ avec $k \in \mathbb{Z}$ donc $a = mk + b$

Or, si l'on considère la division euclidienne de a par m, on a $a = mq + r$ avec $0 \leq r < m$.

D'où $a = mq + r = mk + b$ et donc $mq + r - mk = b$

$$m(q-k) + r = b$$

Et puisque $(q-k) \in \mathbb{Z}$ et $0 \leq r < m$, on en déduit que r est également le reste de la division de b par m.

Ainsi, a et b ont le même reste dans la division euclidienne par m et donc $a \equiv b \ [m]$

Propriétés : Soit m un entier naturel non nul.

(1) Si $a \equiv b\ [m]$ et $b \equiv c\ [m]$ alors $a \equiv c\ [m]$ *(transitivité)*

(2) Si $a \equiv b\ [m]$ et $a' \equiv b'\ [m]$ alors :

- $a + a' \equiv b + b'\ [m]$ et $a - a' \equiv b - b'\ [m]$

  ⇨ En particulier, $na \equiv nb\ [m]$ pour tout $n \in \mathbb{Z}$

- $aa' \equiv bb'\ [m]$ et donc $a^n \equiv b^n\ [m]$ pour tout $n \in \mathbb{N}$

Preuve : (1) Evident par définition (mêmes restes dans la division par m)

(2) On a $a = b + km$ et $a' = b' + k'm$.

- $a + a' = b + km + b' + k'm$

  $= (b + b') + (k + k')m$

Donc $a + a' \equiv b + b'\ [m]$. *Idem pour la soustraction.*

Par ailleurs, $na = n(b + km)$

$= nb + (nk)m$ donc $na \equiv nb\ [m]$

- $aa' = (b + km)(b' + k'm)$

  $= bb' + bk'm + kmb' + kmk'm$

  $= bb' + (bk' + kb' + kk'm)m$

Donc $aa' \equiv bb'\ [m]$. Et la dernière propriété se prouve par récurrence.

II En pratique

1° La base

⇨ Un nombre est toujours congru au reste de la division euclidienne.

⇨ On peut ajouter ou enlever m autant de fois que l'on veut dans une congruence modulo m *(et le plus petit nombre positif que l'on obtient au final est le reste de la division euclidienne)*

En effet, $m \equiv 0\ [m]$ et donc $k \times m \equiv 0\ [m]$

Ex : $x \equiv 18\ [7]$ devient $x \equiv 11\ [7] \equiv 4\ [7]$

$28x - 13 \equiv 11\ [5]$ devient $3x + 2 \equiv 1\ [5]$

$3x \equiv 1 - 2\ [5]$ c'est-à-dire $3x \equiv -1\ [5] \equiv 4\ [5]$

Attention : si $7x \equiv 4\ [5]$ alors $2x \equiv 4\ [5]$ mais on ne peut pas dire que $x \equiv 2\ [5]$ ensuite !

En effet, $2x \equiv 4\ [5]$ signifie que $2x = 4 + 5k$. Et donc $x = 2 + 2{,}5k$

2° La disjonction des cas

Méthode déjà vue dans le chapitre précédent mais qui gagne ici en praticité : au lieu d'écrire explicitement les toutes les divisions euclidiennes possibles en fonction des restes, on va faire des tableaux de congruences.

Ex : Soit n un entier naturel non nul.
1° Montrer que $n(n^2+5)$ est divisible par 3.
2° Déterminer les entiers n pour lesquels $n(n^2+5)$ est divisible par 7.

1° Faisons un tableau des congruences modulo 3 :

n	0	1	2
n^2	0	1	4
n^2+5	2	0	0
$n(n^2+5)$	0	0	0

Ainsi, pour tout $n \in \mathbb{N}$, $n(n^2+5) \equiv 0\ [3]$.

Autrement dit, $\forall n \in \mathbb{N}, 3 | n(n^2+5)$.

⇨ Cela revient à écrire les égalités des trois cas $n = 3p$, $n = 3p+1$ et $n = 3p+2$

2° Même chose avec des congruences modulo 7 :

n	0	1	2	3	4	5	6
n^2	0	1	4	2	2	4	1
n^2+5	5	6	2	0	0	2	6
$n(n^2+5)$	0	6	4	0	0	3	1

Ainsi, $n(n^2+5)$ est divisible par 7 lorsque $n \equiv 0\ [7]$ ou $n \equiv 3\ [7]$ ou $n \equiv 4\ [7]$

Autrement dit, n doit donc être de la forme $7k$, $7k+3$ ou $7k+4$ où $k \in \mathbb{N}$

Ex : Résoudre $47x \equiv -11\ [4]$

Tout d'abord, $47 \equiv 3\ [4]$ et $-11 \equiv 1\ [4]$ donc cette équation équivaut à $3x \equiv 1\ [4]$.

On procède par disjonction des cas avec un tableau de congruences modulo 4 :

x	0	1	2	3
$3x$	0	3	2	1

La seule possibilité est donc $x \equiv 3\ [4]$.

Autrement dit, $7x \equiv 17\ [4]$ si et seulement si $x = 3+4k$ où $k \in \mathbb{Z}$

3° Avec des puissances

Le travail avec les puissances est courant puisqu'il permet de manipuler aisément des grands nombres.

Ex : Quel est le reste de la division de 25^{2018} par 7 ?

On cherche donc à « résoudre » $25^{2018} \equiv ?\ [7]$

On commence tout d'abord par observer que $25^{2018} \equiv 4^{2018}\ [7]$ car $25 \equiv 4\ [7]$

Etudions donc les congruences modulo 7 des puissances de 4 :

$4^1 \equiv 4\ [7]$

$4^2 \equiv 16\ [7]$

$\equiv 2\ [7]$ (×4)

$4^3 \equiv 8\ [7] \equiv 1\ [7]$ ➔ « 1 » est pratique ! (×4)

Or, $2\,018 = 3 \times 672 + 2$ et donc $4^{2018} = 4^{3\times 672+2}$

$= (4^3)^{672} \times 4^2$

$\equiv 1^{672} \times 2\ [7]$

$\equiv 2\ [7]$

Ainsi, le reste de la division euclidienne de 25^{2018} par 7 est 2.

Remarque 1 : avec les congruences modulo m, les restes possibles sont au nombre de m. On va donc finir par retomber sur un reste déjà rencontré ce qui implique que les choses deviennent cycliques.

Ici, on observe que $4^{3p} \equiv 1\ [7]$, $4^{3p+1} \equiv 4\ [7]$ et $4^{3p+2} \equiv 2\ [7]$.

En effet, on a par exemple $4^{3p+1} = (4^3)^p \times 4^1 \equiv 1^p \times 4\ [7] \equiv 4\ [7]$

Application : Déterminer le reste de la division euclidienne de 2^{630} par 10.

$2^1 \equiv 2\ [10]$ $\quad 2^2 \equiv 4\ [10]$ $\quad 2^3 \equiv 8\ [10]$

$2^4 \equiv 16\ [10] \equiv 6\ [10]$ $\quad 2^5 \equiv 12\ [10] \equiv 2\ [10]$ ➔ *reste déjà rencontré*

On a donc un cycle de longueur 4 :

$2^{4p} \equiv 6\ [10]$, $2^{4p+1} \equiv 2\ [10]$, $2^{4p+2} \equiv 4\ [10]$ et $2^{4p+3} \equiv 8\ [10]$

Or, $630 = 4 \times 157 + 2$ donc $2^{630} \equiv 4\ (10)$

⇨ Ici, le cycle est plus délicat à justifier : $2^{4p} = (2^4)^p \equiv 6^p\ [10]$

Il reste donc à vérifier que $6^p \equiv 6\ [10]$: cela peut se faire par récurrence...

Et à partir de là, $2^{4p+1} = 2^{4p} \times 2^1 \equiv 6 \times 2\ [10] \equiv 2\ [10]$ etc.

Remarque 2 : si on a pu constater que trouver un reste qui vaut 1 est pratique (cela évite de donner explicitement le cycle), trouver -1 est également pratique car une puissance paire fera 1 et sinon -1.

Application : Déterminer le reste de la division euclidienne de 2^{2014} par 17.

$2^1 \equiv 2 \ [17]$

$2^2 \equiv 4 \ [17]$

$2^3 \equiv 8 \ [17]$

$2^4 \equiv 16 \ [17] \equiv -1 \ [17]$ (et donc $2^8 \equiv (-1)^2 \ [17] \equiv 1 \ [17]$)

Et de là, $2^{2014} = 2^{4\times503+2}$

$= (2^4)^{503} \times 2^2$

$\equiv (-1)^{503} \times 4 \ [17]$

$\equiv -4 \ [17]$

$\equiv 13 \ [17]$

Remarque 3 : quel est le chiffre des unités de 9^{543} ?

Cela revient à chercher le reste dans la division euclidienne par 10 !

$9^{543} \equiv (-1)^{543} \ [10]$

$\equiv -1 \ [10]$

$\equiv 9 \ [10]$

III Critères de divisibilité

Soit a un nombre entier.
L'écriture décimale de a est « $a_n a_{n-1} \dots a_3 a_2 a_1 a_0$ » où $a_i \in [\![0\,;9]\!], \forall i \in [\![0\,;n]\!]$.

a_0 est le chiffre des unités, a_1 le chiffre des dizaines, etc. On peut donc écrire :

$$a = a_0 + a_1 \times 10^1 + a_2 \times 10^2 + a_3 \times 10^3 + \cdots + a_n \times 10^n = \sum_{i=0}^{n} a_i \times 10^i$$

Divisibilité par 2 :

On observe que $10 \equiv 0 \ [2]$ donc $10^i \equiv 0 \ [2]$

Ainsi, $a_i \times 10^i \equiv a_i \times 0 \ [2] \equiv 0 \ [2]$

De là, $a \equiv a_0 + 0 + 0 + 0 + \cdots + 0 \ [2]$

Autrement dit, $a \equiv a_0 \ [2]$

Donc a est divisible par 2 si son chiffre des unités a_0 est divisible par 2

Divisibilité par 3 :

On observe que $10 \equiv 1 \ [3]$ donc $10^i \equiv 1 \ [3]$

Ainsi, $a_i \times 10^i \equiv a_i \times 1 \ [3] \equiv a_p \ [3]$

De là, $a \equiv a_0 + a_1 + a_2 + a_3 + \cdots + a_n \ [3]$

Donc a est divisible par 3 si la somme de ses chiffres est divisible par 3

On peut s'amuser à chercher d'autres règles, mais toutes ne sont pas vraiment exploitables…

Divisibilité par 11 :

On observe que $10 \equiv 10 \ [11] \equiv -1 \ [11]$ donc $10^i \equiv (-1)^i \ [11]$

Ainsi, $a_i \times 10^i \equiv a_i \times (-1)^i \ [11]$

De là, $a \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n \, a_n \ [11]$

Donc a est divisible par 11 si la somme $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n \, a_n$ est divisible par 11.

Autrement dit, a est divisible par 11 si la somme alternée des chiffres est divisible par 11, à partir de celui des unités.

Ex : $5\,381 \equiv 1 - 8 + 3 - 5 \ [11]$

$\equiv -8 \ [11]$

$\equiv 3 \ [11]$

Le reste de la division euclidienne de 5381 par 11 est 3 : 5 381 n'est pas divisible par 11

$602\,591 \equiv 1 - 9 + 5 - 2 + 0 - 6 \ [11]$

$\equiv -11 \ [11]$

$\equiv 0 \ [11]$

Donc 602 591 est divisible par 11.

Exercice : démontrer qu'un nombre est divisible par 7 si la différence entre son nombre de dizaines et le double de son chiffre des unités est divisible par 7.

Soit a le nombre initial et notons b « *la différence entre son nombre de dizaines et le double de son chiffre des unités est divisible par 7* ».
On a donc $b = \dfrac{a - a_0}{10} - 2a_0$

On veut montrer que $a \equiv 0 \ [7] \iff b \equiv 0 \ [7]$

Pour travailler avec des congruences, il faut préalablement se débarrasser de la division par 10…

On a $10b = a - a_0 - 20a_0 = a - 21a_0$

Supposons que $a \equiv 0 \quad [7]$

On a donc $10b \equiv a - 21a_0 \quad [7]$

$3b \equiv 0 - 0a_0 \quad [7]$

$3b \equiv 0 \quad [7]$

$5 \times 3b \equiv 5 \times 0 \quad [7]$

$15b \equiv 0 \quad [7]$

$b \equiv 0 \quad [7]$

Réciproquement, supposons que $b \equiv 0 \quad [7]$

$10b \equiv 0 \quad [7]$

$a - 21a_0 \equiv 0 \quad [7]$

$a - 0a_0 \equiv 0 \quad [7]$

$a \equiv 0 \quad [7]$

Remarque : un nombre est divisible par 7 si la somme de son nombre de dizaines et le quintuple de son chiffre des unités est divisible par 7…

En effet, $-2a_0 \equiv 5a_0 \quad [7]$