Arithmétique – Partie 4 : Congruences

Savoir.
- ☐ Comprendre la définition de la congruence.
- ☐ Connaître le petit théorème de Fermat.

Savoir-faire.
- ☐ Savoir faire des calculs modulo n.

Congruences

Définition. Soient a et b deux entiers et un entier naturel $n \geqslant 2$. On dit que ***a* est congru à *b* modulo *n*** si n divise la différence $(b-a)$. On note alors :

$$\boxed{a \equiv b\ [n]}$$

Remarques.
- $a \equiv b\ [n]$ revient à dire que les restes de a et de b dans la division euclidienne par n sont les mêmes. Cela veut aussi dire que a et b ne diffèrent que d'un multiple de n, ce qui s'écrit $b = a + kn,\ k \in \mathbb{Z}$.
C'est ainsi que $13 \equiv 8 \equiv 3 \equiv -2\ [5]$ puisque tous ces nombres ne diffèrent entre eux que de multiples de 5.
- On voit parfois dans les livres la notation $a \equiv b \pmod{n}$.
- $a \equiv 0\ [n]$ signifie que $n|a$.

Exemples.
- $65 \equiv 2\ [7]$. En effet 7 divise $65 - 2 = 63$ (ou encore $65 = 7 \times 9 + \mathbf{2}$).
- $13\,145 \equiv 165 \equiv 5\ [10]$. En fait un nombre entier est congru à un autre modulo 10 s'ils se terminent par le même chiffre.
- $n \equiv 0\ [2]$ signifie que n est pair, et $n \equiv 1\ [2]$ que n est impair.
Il n'y a donc que 2 possibilités modulo 2 : être congru à 0 ou à 1. De même il n'y a que trois possibilités modulo 3 : être congru à $0, 1$ ou 2 (ou encore $0, 1$ et -1 car $-1 \equiv 2\ [3]$!).
De manière générale, il y a n possibilités modulo n.

Calculs

Les congruences sont bien adaptées aux additions, soustractions et aux multiplications : autrement dit, on peut y faire de l'arithmétique.

Les règles de calcul. Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors :

$$\boxed{a + c \equiv b + d\ [n] \quad \text{(addition)}}$$

et aussi

$$a - c \equiv b - d\ [n] \quad \text{(soustraction)}$$

enfin

$$\boxed{ac \equiv bd\ [n] \quad \text{(multiplication)}}$$

Attention. Il n'est pas question de parler d'une éventuelle opération de division dans le monde du *modulo* ! En effet, ce monde se préoccupe exclusivement des nombres **entiers** ! On s'échapperait de ce monde merveilleux si on se hasardait à y tenter de la division... Par exemple il serait **extrêmement FAUX** de dire que :

$$2 \equiv 12\,[10] \quad \Longrightarrow \quad \cancel{\frac{2}{12} \equiv 1\,[10]}$$

Aussi on ne peut pas simplifier, par exemple ci-dessous diviser par 2 n'a pas de sens :

$$6 \equiv 2\,[4] \quad \cancel{\Longrightarrow \quad 3 \equiv 1\,[4]}$$

Démonstration des règles de calcul.

— $n|(b-a)$ et $n|(d-c)$, donc n divise l'addition $(b-a)+(d-c)=(b+d)-(a+c)$ (d'où la règle d'addition) et la soustraction $(b-a)-(d-c)=(b-d)-(a-c)$ (d'où la règle de soustraction).

— Pour la multiplication, $n|(b-a)$ donc $n|d(b-a)=db-da$ d'une part ; et $n|(d-c)$ donc $n|a(d-c)=ad-ac$ d'autre part. Par addition, $n|db-da+ad-ac=db-ac$ d'où la règle de multiplication.

Corollaire. Si $a \equiv b\,[n]$, alors pour tout entier l : $la \equiv lb\,[n]$ et pour tout entier k positif, on a :

$$\boxed{a^k \equiv b^k\,[n]}$$

Exemples.

— Commençons par déterminer si le nombre $4^{48}-1$ est ou non un multiple de 5.
Il s'agit de voir si $4^{48}-1 \equiv 0\,[5]$ est vraie.
Puisque $4^2=16=3\times 5+1$, on obtient $4^2 \equiv 1\,[5]$. On passe cette égalité à la puissance 24 (d'après le corollaire) puis on retranchera 1 (d'après les règles de soustraction) :

$$4^2 \equiv 1\,[5] \Longrightarrow (4^2)^{24} \equiv 1^{24}\,[5] \Longleftrightarrow 4^{48} \equiv 1\,[5] \Longleftrightarrow 4^{48}-1 \equiv 0\,[5]$$

Ainsi le nombre $4^{48}-1$ est bien un multiple de 5. Parviens-tu, en utilisant les congruences modulo 2, à déterminer s'il se termine par 0 ou par 5 ?

— Cherchons à présent quel est le chiffre des unités du nombre $3^{240}+7^{240}$. Il s'agit de déterminer la congruence de ce nombre modulo 10.
Tout d'abord, $3^2=9$ est congru à -1 modulo 10.
Ce sera notre point de départ :

$$3^2 \equiv -1\,[10] \Longrightarrow (3^2)^{120} \equiv (-1)^{120}\,[10] \Longleftrightarrow 3^{240} \equiv 1\,[10]$$

On rappelle que calculer $(-1)^k$ est facile : c'est $+1$ si k est pair et -1 si k est impair. Passons à la puissance de 7 : puisque $7^2=49$ est congru à -1 modulo 10, on obtient de même :

$$7^2 \equiv -1\,[10] \Longrightarrow (7^2)^{120} \equiv (-1)^{120}\,[10] \Longleftrightarrow 7^{240} \equiv 1\,[10]$$

Ainsi par addition, $3^{240}+7^{240} \equiv 2\,[10]$ ce qui signifie que son chiffre des unités est 2.

Exercice.

1. Montrer que pour tout entier naturel n, le nombre $4^{3n}-4^n$ est un multiple de 5.
2. Montrer que "$13|(5^{2n}+3^{3n}) \Longleftrightarrow n$ est impair".

Petit théorème de Fermat

Le calcul des congruences est particulièrement intéressant lorsque le modulo choisi est lui-même un nombre premier. C'est notamment ce qu'illustre le petit théorème de Fermat :

Petit théorème de Fermat (1 640). Si p est un nombre premier, alors pour tout entier x on a :

$$\boxed{x^p \equiv x\ [p]}$$

En particulier, **si x n'est pas un multiple de** p, alors :

$$\boxed{x^{p-1} \equiv 1\ [p]}$$

Exemple. Calculons $5^{2\,022}$ modulo 13.

— D'après le petit théorème de Fermat, 13 étant premier et 5 n'étant pas un multiple de 13, on sait que $5^{12} \equiv 1\ [13]$.

— Par ailleurs la division euclidienne de 2 022 par 12 est $= 2\,022 = 12 \times 168 + 6$. Donc en passant à la puissance 168 on obtient $5^{12\times 168} = (5^{12})^{168} \equiv 1\ [13]$.

— Or $5^2 \equiv 25 \equiv -1\ [13]$, ainsi $5^6 = (5^2)^3 \equiv (-1)^3 \equiv -1\ [13]$.
Par multiplication, on obtient : $5^{2\,022} \equiv 5^{12\times 168} \times 5^6 \equiv 1 \times (-1) \equiv -1 \equiv 12\ [13]$.

Exercice. Calculer 4^{253} modulo 11 et 25^{71} modulo 7.