Congruence

Lors du premier chapitre d'arithmétique, nous avons rencontré la notion de division euclidienne, dont nous rappelons à tout hasard la définition. Si l'on se donne deux entiers relatifs a et b, alors il existe un unique couple d'entiers (q,r) vérifiant $a = bq + r$ et $0 \leqslant r < b$.

1 Congruence modulo n

Définition 1 : Soit n un entier naturel non nul, a et b deux entiers relatifs. On dit que a est congrus à b modulo n si a et b ont le même reste dans la division euclidienne par n.

On écrit $a \equiv b\,[n]$

■ **Exemple 1 :** $13 \equiv 21\,[4]$. En effet, la division euclidienne de 21 par 4 est $21 = 4 \times 5 + 1$ et celle de 13 par 4 est $13 = 4 \times 3 + 1$. 13 et 21 ont donc pour reste 1 dans la division euclidienne par 4. ■

Cette définition est évidemment motivée par l'existence et l'unicité de la division euclidienne. Plutôt que d'affirmer qu'un entier n peut s'écrire sous une des formes $3k$, $3k+1$ ou $3k+2$, pour k un certain entier, on peut également dire que l'on se trouve dans l'une des situations suivantes : $n \equiv 0\,[3]$, $n \equiv 1\,[3]$ ou $n \equiv 2\,[3]$.

D'une manière plus générale...

Propriété 1 : Soit a un entier relatif et n un entier naturel non nul. Il existe un unique $m \in \{0; 1; 2; \ldots; n\}$ tel que $a \equiv m\,[n]$.

Démonstration 1.1 : Le m en question n'est autre que le reste de la division euclidienne de a par n. □

Il existe toutefois une autre manière, sans doute plus commode de définir les congruences.

Propriété 2 : Soit n un entier naturel non nul, a et b deux entiers relatifs.

Alors $a \equiv b\,[n]$ si et seulement si $(a-b)$ est un multiple de n.

En particulier, a est un multiple de n si et seulement si $a \equiv 0\,[n]$.

Démonstration 1.2 : Soit n un entier naturel non nul, a et b deux entiers relatifs. Écrivons alors la division euclidienne de a et b par n

- Il existe deux entiers relatifs q et r tels que $a = nq + r$ et $0 \leqslant r < n$
- Il existe deux entiers relatif q' et r' tels que $b = nq' + r$ et $0 \leqslant r' < n$

Nous raisonnerons par double implication

- Supposons que $a \equiv b\,[n]$. On a alors $r = r'$. Ainsi, $(a-b) = nq + r - (nq' + r) = n(q - q')$. $(a-b)$ est donc bien un multiple de n.
- Réciproquement, supposons que $(a-b)$ est un multiple de n. Alors il existe un entier relatif k tel que $a - b = kn$. Or, $a - b = nq + r - nq' - r' = n(q-q') + r - r'$ et donc $kn = n(q-q') + r - r'$ ce qui entraîne $n(k - q + q') = r - r'$. $r - r'$ est donc un multiple de n. Seulement, on a $-n < r - r' < n$. Il en vient que $r - r' = 0$ et donc que $r = r'$.

□

■ **Exemple 2 :** On a $414 \equiv 144\,[27]$. En effet, $414 - 144 = 270$, qui est un multiple de 27. ■

2 Compatibilité de la congruence avec les opérations

Propriété 3 — Relation d'équivalence. : Soit n un entier naturel non nul

- Pour tout entier relatif a, $a \equiv a\,[n]$. La relation de congruence est **réflexive**.
- Pour tous entiers relatifs a et b, si $a \equiv b\,[n]$, alors $b \equiv a\,[n]$. La relation de congruence est **symétrique**.
- Pour tous entiers relatifs a, b et c, si $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors $a \equiv c\,[n]$. La relation de congruence est **transitive**.

On dit que la relation de congruence modulo n est une relation d'équivalence sur l'ensemble des entiers relatifs.

Démonstration 2.1 :

- On a $a - a = 0$, qui est bien un multiple de n.
- Si $a \equiv b\,[n]$, alors il existe un entier relatif k tel que $a - b = kn$ et donc $b - a = (-k)n$. $b - a$ est donc un multiple de n. On a donc $b \equiv a\,[n]$
- Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors il existe des entiers relatifs k et k' tels que $a - b = kn$ et $b - c = k'n$. Mais alors, $a - c = a - b + b - c = kn + k'n = (k + k')n$. $a - c$ est donc un multiple de n et donc $a \equiv c\,[n]$

□

Propriété 4 : Soit n un entier naturel non nul, a, b, c et d quatre entiers relatifs

- Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors $a + c \equiv b + d\,[n]$.
- Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors $ac \equiv bd\,[n]$. En particulier, $a^k \equiv b^k\,[n]$ pour tout entier naturel k.
- Si $a \equiv b\,[n]$, alors pour tout entier relatif m, $ma \equiv mb[mn]$

Démonstration 2.2 :

- Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors il existe deux entiers relatifs k et k' tels que $a - b = kn$ et $c - d = k'n$. Ainsi, $a + c - (b + d) = a - b + c - d = kn + k'n = (k + k')n$. Il en vient que $(a + c) - (b - d)$ est un multiple de n. On a donc bien $a + c \equiv b + d\,[n]$.
- Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors il existe deux entiers relatifs k et k' tels que $a - b = kn$ et $c - d = k'n$. On a donc $a = b + kn$ et $c = d + k'n$. Ainsi,

  $$ac - bd = (b + kn)(d + k'n) - bd = bd + bk'n + dkn + kk'n^2 - bd = (bk' + dk + kk'n)n$$

  Le passage aux puissances se montre par récurrence en utilisant la propriété que nous venons de démontrer. Ainsi, $ac - bd$ est un multiple de n. On a donc bien $ac \equiv bd\,[n]$.
- Si $a \equiv b\,[n]$, alors il existe un entier relatif k tel que $a - b = kn$. Mais alors $ma - mb = m(a - b) = mkn = k(mn)$, qui est un multiple de mn. On a donc bien $ma \equiv mb[mn]$

□

Les règles opératoires sur les congruences nous permettent de résoudre plus facilement les questions de divisibilité. En effet, dire qu'un nombre est divisible par un autre, c'est dire qu'il est congrus à 0 modulo ce dernier entier.

■ **Exemple 3 :** Montrons que, pour tout entier naturel n, $2^{3n} - 1$ est un multiple de 7. On sait que pour tout entier naturel n, $2^{3n} = (2^3)^n = 8^n$. Or, $8 \equiv 1\,[7]$. Ainsi, pour tout entier naturel n, $2^{3n} - 1 \equiv 1^n - 1 \equiv 0\,[7]$. $2^{3n} - 1$ est donc bien un multiple de 7. ■

Une des applications les plus courantes des congruences est le raisonnement par disjonction de cas.

■ **Exemple 4 :** Soit n un entier naturel. On souhaite déterminer les valeurs de n pour lesquelles $5n^2+19n-2$ est divisible par 4. On raisonne par disjonction de cas, suivant la congruence de n modulo 4. Notons d'abord que, puisque $5 \equiv 1\,[4]$ et $19 \equiv 3\,[4]$, alors $5n^2 + 19n - 3 \equiv n^2 + 3n - 3\,[4]$

$n \equiv \ldots\,[4]$	0	1	2	3
$n^2 \equiv \ldots\,[4]$	0	1	0	1
$3n \equiv \ldots\,[4]$	0	3	2	1
$n^2 + 3n - 3 \equiv \ldots\,[4]$	-2	-2	0	0

Ainsi, $5n^2 + 19n - 2$ est divisible par 4 si et seulement si $n \equiv 2\,[4]$ ou $n \equiv 3\,[4]$ (ou encore, s'il existe un entier relatif k tel que $n = 4k + 2$ ou $n = 4k + 3$). ■

Il faut toutefois faire attention lorsque l'on manipule des entiers en exposant. Nous disposons pas - à ce stade - de règles qui permettent de simplifier directement les exposants. Une méthode très utile est d'étudier les puissances d'un nombre jusqu'à tomber sur une congruence à 1. A partir de là, les congruences de toutes les puissances de ce nombre peuvent se déduire très facilement.

■ **Exemple 5 :** On souhaite savoir le reste de la division euclidienne de 8^{483} par 5.

D'abord, remarquons que $8 \equiv 3\,[5]$. On a donc $8^{483} \equiv 3^{483}\,[5]$. En revanche, il n'est pas possible d'appliquer un même raisonnement sur le nombre en exposant. Regardons plutôt les premières puissances de 2...

- On a $3^0 = 1$ et donc $3^0 \equiv 1[5]$. Par ailleurs, $3^1 = 3$ et donc $3^1 \equiv 3\,[5]$
- On a $3^2 = 9$ et donc $3^2 \equiv 4\,[5]$.
- On pourrait alors calculer directement 3^3 et déterminer sa congruence modulo 5... Mais épargnons-nous ce souci ! En effet, puisque $3^2 \equiv 4\,[5]$, en multipliant cette relation par 3, on obtient que $3^3 \equiv 12\,[5]$. Or, $12 \equiv 2\,[5]$. Finalement, $3^3 \equiv 2\,[5]$
- On procède de la même manière pour 3^4 : puisque $3^3 \equiv 2\,[5]$, on a alors $3^4 \equiv 6\,[5]$. Or, $6 \equiv 1\,[5]$. Finalement, $3^4 \equiv 1\,[5]$.
- On pourrait alors continuer ainsi. On trouverait $3^5 \equiv 3\,[5]$, $3^6 \equiv 4\,[5]$, $3^7 \equiv 2\,[5]$ et $3^8 \equiv 1\,[5]$

On remarque alors que les congruences sont cycliques, de période 4... En fait, on peut s'arrêter dès que l'on trouve une puissance de 3 congrus à 1 modulo 5 : il s'agit de 3^4.

Pour savoir à quoi est congrus 3^{483} modulo 5, il suffit donc de savoir à quoi est congrus 483 modulo 4.

Or, $483 = 4 \times 120 + 3$. Ainsi, $3^{483} = 3^{4\times120+3} = (3^4)^{120} \times 3^3$. Ainsi,

$$8^{483} \equiv 3^{483} \equiv 3^3 \equiv 2\,[5]$$

Le reste de la division euclidienne de 8^{483} par 5 est 2. ■