**Arithmétique. Cours**

| **Congruence** | |
|---|---|
| **Définition** | Soit $n$ un entier naturel supérieur ou égal à deux.<br>Soient $a$ et $b$ deux entiers relatifs.<br>On dit que $a$ et $b$ sont **congrus** modulo $n$ et on note $a \equiv b(n)$<br>Lorsque de le reste de la vision euclidienne de $a$ par $n$ est égal au reste de la division euclidienne de $b$ par $n$ |
| **Exemple** | $77 = 75 + 2 = 5 * 15 + 2$ Le reste de la division euclidienne de 77 par 5 est 2<br>$22 = 20 + 2 = 5 * 4 + 2$ Le reste de la division euclidienne de 22 par 5 est 2<br>Donc $77 \equiv 22(5)$ |
| **Propriété** | Soient $a$ un entier relatif et $n$ un entier naturel supérieur ou égal à deux<br>$a$ est congru modulo $n$ au reste de la division euclidienne de $a$ par $n$ |
| **Preuve** | |
| $a = bn + r$ avec $0 \leq r < n$<br>$r = 0 * n + r$ avec $0 \leq r < n$<br>Donc $a \equiv r(n)$ | |
| **Théorème** | Soient $a$ et $b$ deux entiers relatifs et $n$ un entier naturel supérieur ou égal à deux.<br>$\boldsymbol{a \equiv b(n) \Leftrightarrow \exists k \in Z \; tq \; a = b + kn}$ |
| **Preuve** | |
| $a \equiv b(n) \Rightarrow \begin{cases} a = qn + r \; avec \; 0 \leq r < n \\ b = q'n + r \; avec \; 0 \leq r < n \end{cases} \Rightarrow a - b = (q - q')n \Rightarrow a = b + (q - q')n$<br><br>Réciproquement : supposons $\exists k \in Z \; tq \; a = b + kn$<br>Soit $r$ le reste de la division euclidienne de $b$ par $n$ : $b = nq + r$ avec $0 \leq r < n$<br>$a = b + kn \Rightarrow a = nq + r + kn \Rightarrow a = n(q + k) + r$ avec $0 \leq r < n.$<br>Donc le reste de la division euclidienne de $a$ par $n$ est aussi $r$ | |
| **Exemple** | Nous avons vu que $77 \equiv 22(5)$<br>En effet $77 = 22 + 5 * 10$ |
| **Remarques** | • Un nombre pair est un nombre congru a $0$ modulo $n$<br>• Un nombre impair est un nombre congru a $1$ modulo $n$<br>• $n$ est un diviseur de $a \; ssi \; a \equiv 0 \; (n)$ |
| **Propriété** | La relation de congruence est une relation d'équivalence.<br>Cela signifie qu'elle est :<br>• **Réflexive** : $\boldsymbol{a \equiv a(n)}$<br>• **Symétrique** : $\boldsymbol{a \equiv b(n) \Leftrightarrow b \equiv a(n)}$<br>• **Transitive** : $\boldsymbol{a \equiv b(n)}$ et $\boldsymbol{b \equiv c(n)}$ alors $\boldsymbol{a \equiv c(n)}$ |
| **Preuve** | |
| $a = a + 0 * n \Rightarrow \boldsymbol{a \equiv a(n)}$ **.** La relation est donc réflexive.<br>$\boldsymbol{a \equiv b(n)} \Rightarrow a = b + k * n \Rightarrow b = a - k * n \Rightarrow \boldsymbol{b \equiv a(n)}$ **.** La relation est donc symétrique.<br>$\boldsymbol{a \equiv b(n)} \Rightarrow a = b + k * n$<br>$\boldsymbol{b \equiv c(n)} \Rightarrow b = c + k' * n$ donc $a = c + k' * n + k * n = c + (k + k') * n \Rightarrow a \equiv c(n)$<br>La relation est donc transitive. | |

| | |
|---|---|
| **Théorème** | La relation de congruence est compatible avec l'addition, la multiplication et les puissances d' entiers. Cela signifie que si $n \geq 2$<br>• $\left.\begin{matrix} a \equiv c(n) \\ b \equiv d(n) \end{matrix}\right\} \Rightarrow a+b \equiv c+d(n)$<br>• $\left.\begin{matrix} a \equiv c(n) \\ b \equiv d(n) \end{matrix}\right\} \Rightarrow ab \equiv cd\ (n)$<br>• $a \equiv b(n) \Rightarrow a^k \equiv b^k(n)$ pour $k \in \mathbb{N}$ |

**Preuve**

- $\left.\begin{matrix} a \equiv c(n) \\ b \equiv d(n) \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} a \equiv c+kn \\ b \equiv d+k'n \end{matrix}\right\} \Rightarrow a+b = c+d+\left(k+k^{'}\right)n \Rightarrow a+b \equiv c+d(n)$

- $\left.\begin{matrix} a \equiv c(n) \\ b \equiv d(n) \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} a \equiv c+kn \\ b \equiv d+k'n \end{matrix}\right\} \Rightarrow ab = (c+kn)\left(d+k^{'}n\right) = cd+n(k^{'}c+kd+kk^{'}n^{'}) \Rightarrow ab \equiv cd\ (n)$

- Demonstration par recurrence sur $k$
  Pour $k = 1$, c'est vérifié car $a \equiv b(n)$
  Supposons que $a^k \equiv b^k(n)$ alors $a^{k+1} = a * a^k \equiv b * b^k\ (d'après\ le\ point\ 2)$
  Et donc $a^{k+1} \equiv b^{k+1}(n)$

| | |
|---|---|
| **Exemple** | $62 \equiv 2(5)$<br>$78 \equiv 3(5)$<br>Donc $62 * 78 \equiv 6(5)$ ; $62+78 \equiv 5(5)$ ; $62^2 \equiv 4(5)$ |