Exemple fondamental. Congruences.

$a, b, m \in \mathbb{Z}$

$a \equiv b \mod m$ si $a-b$ divisible par m, c-à-d $a-b = km$, $k \in \mathbb{Z}$.

équivalence : (R) : $a-a=0$ divisible par m ($\forall m$) donc $a \equiv a \mod m$

(S) : $a-b = km \Leftrightarrow b-a = (-k)m$ donc $a \equiv b \mod m \Leftrightarrow b \equiv a \mod m$.

(TR) : $a-b = km$, $b-c = k'm$ alors $a-c = a-b+b-c = km + k'm = (k+k')m$

donc $a \equiv b \mod m$ et $b \equiv c \mod m \Rightarrow a \equiv c \mod m$.

$Cl(a) = \{b \mid a-b = km\ \exists k \in \mathbb{Z}\} = \{b \mid b = a + km,\ k \in \mathbb{Z}\} = \{a + km,\ k \in \mathbb{Z}\}$

$= \boxed{a + m\mathbb{Z}}$.

Rem. $a-b = km \Leftrightarrow a-b = (-k)(-m)$ $a \equiv b \mod m$ si $a \equiv b \mod -m$.

donc on peut supposer $m \geq 0$.

Ensemble quotient : $\dfrac{\mathbb{Z}}{m\mathbb{Z}} = \{a + m\mathbb{Z},\ a \in \mathbb{Z}\}$ il a m élmts.

$= \{0 + m\mathbb{Z},\ 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}$

$= \{m\mathbb{Z},\ 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}$ → restes possibles.

$= \{[0]_m, [1]_m, \ldots, [m-1]_m\}$

$= \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.

Th. opérations sur les congruences :

$a \equiv a' \mod m$, $b \equiv b' \mod m'$ alors

$a + b \equiv a' + b' \mod m$, $ab \equiv a'b' \mod m$.

Conséquence, on peut faire les op. sur les classes en faisant les opérations sur deux représentants :

$[1]_m + [2]_m = [3]_m$ etc.

Ex. 2.59. $\forall k \in \mathbb{N}$, on a

$10^k \equiv 1 \mod 3$ car $10^k - 1 = (10-1)(10^{k-1} + 10^{k-2} + \ldots) = \underset{3}{\underline{9}}\,(10^{k-1} + 10^{k-2} + \ldots + 10 + 1)$

donc aussi $10^k \equiv 1 \mod 9$.

$10^k \equiv (-1)^k \mod 11$: par récurrence : $k=0$: $10^0 = 1 \equiv (-1)^0 = 1 \mod 11$ ok.

$10^{k+1} \equiv 10 \cdot 10^k \overset{(R)}{\equiv} (-1)(-1)^k \equiv (-1)^{k+1} \mod 11$.

$n = a_k \cdot 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$.

donc $n \overset{(2)}{\equiv} 0+0+\cdots+0+a_0 \equiv a_0 \mod 2.$

$n \equiv 0+\cdots+0+a_0 \mod 5$

$n \equiv 0+\cdots+10a_1+a_0 \mod 4$ etc. on retrouve les critères de divisibilité.