Chapitre 6
Relations de congruences modulo n

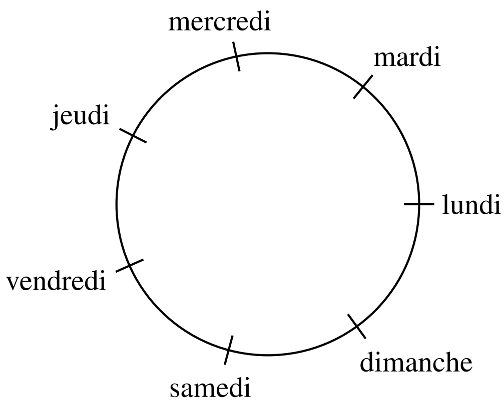
1 Congruences modulo n dans $\mathbb{Z}$

Définition 1. Soit n un entier naturel non nul et a, b deux entiers (relatifs). On dit que a *est congru à* b *modulo* n, que l'on note $a \equiv b \pmod{n}$, si et seulement si $a - b$ est divisible par n.
L'expression $a \equiv b \pmod{n}$ est alors une *congruence* et n est son *module*.

Exemples 1.1.

1. Relation de congruence modulo 2 (cas $n = 2$) :
   Donnez des entiers congrus à 4 modulo 2 :
   $4 \equiv \cdots \pmod{2}$ car $\qquad$ $4 \equiv \cdots \pmod{2}$
   $4 \equiv \cdots \pmod{2}$ car $\qquad$ $4 \equiv \cdots \pmod{2}$
   $4 \equiv \cdots \pmod{2}$ car $\qquad$ $4 \equiv \cdots \pmod{2}$
   Remarque : Un entier n est pair si et seulement si $n \equiv \quad \pmod{2}$.

   Comment pourrait-on alors caractériser les entiers impairs ?
   Un entier n est impair si et seulement si $n \equiv \quad \pmod{2}$.
2. Relation de congruence modulo 7 (cas $n = 7$) :
   Aujourd'hui nous sommes . (Compléter avec le jour de la semaine où a lieu le cours)
   Quel jour de la semaine serons-nous dans 2 413 jours ?



3. $125 \equiv 4 \pmod{11}$ car $125 - 4 = 121$ et $11 \mid 121$.
4. Soit $n \in \mathbb{N}^*$ quelconque. Alors pour tout $a \in \mathbb{Z}$, on a $a \equiv a \pmod{n}$ car $n \mid 0$.
5. Pour tous $a, b \in \mathbb{Z}$, $a \equiv b \pmod{1}$ car $1 \mid a - b$.
6. Soit $n = 3$. Alors $\quad \equiv 0 \pmod{3}$, $\quad \equiv 1 \pmod{3}$, $\quad \equiv 2 \pmod{3}$, $3 \equiv \quad \pmod{3}$, $\quad \equiv 1 \pmod{3}$.

Notation : Si $n \nmid a - b$, on écrit $a \not\equiv b \pmod{n}$ et on dit que a est *non congru à* b *modulo* n.

1.2 Remarques. Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. Alors :

1. $a \equiv b \pmod{n} \iff n \mid a - b \iff \exists\, k \in \mathbb{Z} \,/\, a - b = kn \iff \exists\, k \in \mathbb{Z} \,/\, a = b + kn$.
2. $a \equiv 0 \pmod{n}$ si et seulement si $n \mid a$.
3. $a \equiv b \pmod{n}$ si et seulement si $a - b \equiv 0 \pmod{n}$.

Proposition 1. *Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. Alors $a \equiv b \pmod{n}$ si et seulement si a et b ont même reste dans la division euclidienne par n.*

Définition 2. Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Soit r le reste de la division euclidienne de a par n, c'est-à-dire que r est donné par $a = nq + r$ avec $0 \leq r < n$ (en particulier $a \equiv r \pmod{n}$). On appelle r le *résidu de a modulo n* ; c'est le plus petit entier naturel auquel a est congru modulo n.

Exemples 1.3.

1. $125 \equiv 4 \pmod{11}$ avec $0 \leq 4 < 11$, par conséquent 4 est le résidu de 125 modulo 11.
   On remarquera que la division euclidienne de 125 par 11 s'écrit $125 = 11 \times 11 + 4$, avec $0 \leq 4 < 11$
2. $35 \equiv -1 \pmod{12}$ mais -1 n'est pas le résidu de 35 modulo 12 puisque $-1 < 0$. On a $35 = 12 \times 2 + 11$ avec $0 \leq 11 < 12$, par conséquent 11 est le résidu de 35 modulo 12.
3. *Exercice : 1 738 est-il congru à 219 modulo 7 ?*

   $1^{ère}$ *méthode* :

   $2^{ème}$ *méthode* :

2 Propriétés

Théorème 2.1. *Soient $n \in \mathbb{N}^*$. Alors on a :*

1. *La relation de congruence modulo n est réflexive : $a \equiv a \pmod{n}$ $\forall a \in \mathbb{Z}$.*
2. *La relation de congruence modulo n est symétrique :*
   si $a \equiv b \pmod{n}$, alors $b \equiv a \pmod{n}$ $\forall a, b \in \mathbb{Z}$.
3. *La relation de congruence modulo n est transitive :*
   si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$ $\forall a, b, c \in \mathbb{Z}$.

2.2 Remarques.

1. *La relation de congruence modulo n est donc une relation d'équivalence dans $\mathbb{Z}$.*
2. *On dira indifféremment que a est congru à b $\pmod{n}$, ou que b est congru à a $\pmod{n}$, ou encore que a et b sont congrus $\pmod{n}$.*

Théorème 2.3. *Soient $n \in \mathbb{N}^*$ et $a, a', b, b' \in \mathbb{Z}$ tels que*

$$\left\{ \begin{array}{l} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{array} \right. .$$

Alors :

1. *Pour tous x, y dans $\mathbb{Z}$, $xa + yb \equiv xa' + yb' \pmod{n}$ (linéarité de la relation de congruence). En particulier, $a + b \equiv a' + b' \pmod{n}$.*
2. *$ab \equiv a'b' \pmod{n}$.*
3. *Conséquence : pour tout $m \in \mathbb{N}$, $a^m \equiv (a')^m \pmod{n}$.*

Exemples 2.4.

1. Si $a \equiv 2, \pmod{5}$ et $b \equiv 3, \pmod{5}$ alors

$$\begin{array}{rl} & -3a + 4b \equiv -3 \times 2 + 4 \times 3 \pmod{5} \\ \iff & -3a + 4b \equiv 6 \pmod{5} \\ \iff & -3a + 4b \equiv 1 \pmod{5} \end{array}$$

2. On souhaite déterminer le résidu de 34^4 modulo 7. Déterminer d'abord le résidu de 34 modulo 7 :

   Alors $34^2 \equiv \quad \pmod{7} \iff 34^2 \equiv \quad \pmod{7}$.
   Et donc $34^4 \equiv \quad \pmod{7}$.
   Le résidu de 34^4 modulo 7 est donc . On pourra noter $res_7(34^4) = 1$.

3 Application : critères de divisibilité

Théorème 3.1.

1. *Un entier naturel est divisible par 9 si et seulement si la somme de ses chiffres, en système décimal, est divisible par 9.*
2. *Un entier naturel est divisible par 3 si et seulement si la somme de ses chiffres, en système décimal, est divisible par 3.*

Démonstration :

Théorème 3.2. *Critère de divisibilité par 11 :*

Exemples 3.3.

1. Les entiers 201 520 142 013 et 201 420 132 012 sont-ils divisibles par 11 ?

2. Déterminer le chiffre décimal x pour que le nombre $1\ 72x\ 321$ soit divisible par 11.
   Même question avec le nombre $x81\ 817$.