Proposition :

Soit a, a', b et b' quatre entiers relatives vérifiant les relations suivantes :

$a \equiv a' \pmod{c}$; $b \equiv b' \pmod{c}$

On a les propriétés algébriques suivantes :

1. $a+b \equiv a'+b' \pmod{c}$
2. $a-b \equiv a'-b' \pmod{c}$
3. $a \cdot b \equiv a' \cdot b' \pmod{c}$
4. $a^n \equiv a'^n \pmod{c}$

Démonstration :

Puisque $a \equiv a' \pmod{c}$, il existe un entier k vérifiant :

$a = a' + k \cdot c$

De même, il existe un entier k' tel que :

$b' = b' + k' \cdot c$

1. Ainsi, on a :

$$a+b = \big(a'+k\cdot c\big) + \big(b'+k'\cdot c\big)$$
$$= a'+b'+k\cdot c+k'\cdot c = a'+b'+\big(k+k'\big)\cdot c$$

Ainsi, on a : $a+b \equiv a'+b' \pmod{c}$

2. Ainsi, on a :

$$a-b = \big(a'+k\cdot c\big) - \big(b'+k'\cdot c\big)$$
$$= a'-b'+k\cdot c-k'\cdot c = a'-b'+\big(k-k'\big)\cdot c$$

Ainsi, on a : $a-a' \equiv b-b' \pmod{c}$

3. De même, on a :

$$a \cdot b = \big(a'+k\cdot c\big)\cdot\big(b'+k'\cdot c\big)$$
$$= a'\cdot b' + a'\cdot k'\cdot c + k\cdot c\cdot b' + k\cdot k'\cdot c^2$$
$$= a'\cdot b' + c\cdot\big(b\cdot k' + k\cdot b' + k\cdot k'\cdot c\big)$$

On en déduit : $a\cdot b \equiv a'\cdot b' \pmod{c}$

4. Considérons la propriété $\mathcal{P}_n$ définie pour tout entier naturel n définie par :

$\mathcal{P}_n$: "$a^n \equiv a'^n \pmod{c}$"

Montrons, à l'aide d'un raisonnement par récurrence, que pour tout entier naturel n la propriété $\mathcal{P}_n$ est vraie :

- **Initialisation :**

$a^0 = 1 \equiv 1 \pmod{c}$; $a'^0 = 1 \equiv 1 \pmod{c}$

On vient d'établir que $\mathcal{P}_0$ est vraie.

- **Hérédité :**

Supposons la propriété $\mathcal{P}_n$ réalisée pour un entier naturel n quelconque. C'est à dire qu'on a l'hypothèse par récurrence :

$a^n \equiv a'^n \pmod{c}$

Les entiers a et a' vérifient également :

$a \equiv a' \pmod{c}$

Par multiplication de ces deux équivalences, on obtient :

$a^n \cdot a \equiv a'^n \cdot a' \pmod{c} \Longrightarrow a^{n+1} \equiv a'^{n+1} \pmod{c}$

On vient d'établir la propriété $\mathcal{P}_{n+1}$.

- **Conclusion :**

On vient d'établir que la propriété $\mathcal{P}_n$ est initialisée pour $n=0$ et vérifie la propriété d'hérédité. A l'aide d'un raisonnement par récurrence, on vient d'établir que la propriété $\mathcal{P}_n$ est réalisée pour tout entier naturel n.

Proposition :

Soit a, a', b et b' quatre entiers relatives vérifiant les relations suivantes :

$a \equiv a' \pmod{c}$; $b \equiv b' \pmod{c}$

On a les propriétés algébriques suivantes :

1. $a+b \equiv a'+b' \pmod{c}$
2. $a-b \equiv a'-b' \pmod{c}$
3. $a \cdot b \equiv a' \cdot b' \pmod{c}$
4. $a^n \equiv a'^n \pmod{c}$

Démonstration :

Puisque $a \equiv a' \pmod{c}$, il existe un entier k vérifiant :

$a = a' + k \cdot c$

De même, il existe un entier k' tel que :

$b' = b' + k' \cdot c$

1. Ainsi, on a :

$$a+b = \big(a'+k\cdot c\big) + \big(b'+k'\cdot c\big)$$
$$= a'+b'+k\cdot c+k'\cdot c = a'+b'+\big(k+k'\big)\cdot c$$

Ainsi, on a : $a+b \equiv a'+b' \pmod{c}$

2. Ainsi, on a :

$$a-b = \big(a'+k\cdot c\big) - \big(b'+k'\cdot c\big)$$
$$= a'-b'+k\cdot c-k'\cdot c = a'-b'+\big(k-k'\big)\cdot c$$

Ainsi, on a : $a-a' \equiv b-b' \pmod{c}$

3. De même, on a :

$$a \cdot b = \big(a'+k\cdot c\big)\cdot\big(b'+k'\cdot c\big)$$
$$= a'\cdot b' + a'\cdot k'\cdot c + k\cdot c\cdot b' + k\cdot k'\cdot c^2$$
$$= a'\cdot b' + c\cdot\big(b\cdot k' + k\cdot b' + k\cdot k'\cdot c\big)$$

On en déduit : $a\cdot b \equiv a'\cdot b' \pmod{c}$

4. Considérons la propriété $\mathcal{P}_n$ définie pour tout entier naturel n définie par :

$\mathcal{P}_n$: "$a^n \equiv a'^n \pmod{c}$"

Montrons, à l'aide d'un raisonnement par récurrence, que pour tout entier naturel n la propriété $\mathcal{P}_n$ est vraie :

- **Initialisation :**

$a^0 = 1 \equiv 1 \pmod{c}$; $a'^0 = 1 \equiv 1 \pmod{c}$

On vient d'établir que $\mathcal{P}_0$ est vraie.

- **Hérédité :**

Supposons la propriété $\mathcal{P}_n$ réalisée pour un entier naturel n quelconque. C'est à dire qu'on a l'hypothèse par récurrence :

$a^n \equiv a'^n \pmod{c}$

Les entiers a et a' vérifient également :

$a \equiv a' \pmod{c}$

Par multiplication de ces deux équivalences, on obtient :

$a^n \cdot a \equiv a'^n \cdot a' \pmod{c} \Longrightarrow a^{n+1} \equiv a'^{n+1} \pmod{c}$

On vient d'établir la propriété $\mathcal{P}_{n+1}$.

- **Conclusion :**

On vient d'établir que la propriété $\mathcal{P}_n$ est initialisée pour $n=0$ et vérifie la propriété d'hérédité. A l'aide d'un raisonnement par récurrence, on vient d'établir que la propriété $\mathcal{P}_n$ est réalisée pour tout entier naturel n.

Proposition :

Deux entiers sont congrus entre eux modulo c si, et seulement, si leur différence est un multiple de c.

Démonstration :

La division euclidienne des entiers b et a permettent d'obtenir les couples $(q\,;r)$ et $\left(q'\,;r'\right)$ tels que :
$a=q\cdot c+r$ où $0\leqslant r\leqslant|c|$; $b=q'\cdot c+r'$ où $0\leqslant r'\leqslant|c|$

- $\Longrightarrow$:
  Supposons que le nombre $(a-b)$ est un multiple de c : il existe un entier k vérifiant :
  $a-b=k\cdot c$
  Le nombre $(a-b)$ peut s'écrire :
  $$a-b=\left(q-q'\right)\cdot c+\left(r-r'\right)$$
  $$k\cdot c=\left(q-q'\right)\cdot c+\left(r-r'\right)$$
  $$k\cdot c-\left(q-q'\right)\cdot c=\left(r-r'\right)$$
  $$r-r'=\left[k-\left(q-q'\right)\right]\cdot c$$
  On vient de montrer que le nombre $(r-r')$ est un multiple de c.

  Des propriétés des restes, on écrit :
  $$\left\{\begin{array}{l}0\leqslant r\leqslant|c|\\0\leqslant r'<|c|\end{array}\right.\Longrightarrow\left\{\begin{array}{r}0\leqslant r\leqslant|c|\\-|c|<r'\leqslant 0\end{array}\right.$$
  On en déduit l'encadrement suivant :
  $-|c|<r-r'<|c|$

  Dans l'intervalle $\left]-|c|\,;|c|\right[$, le seul multiple de c est 0 :
  $r-r'=0\quad\Longrightarrow\quad r=r'$

- $\Longleftarrow$:
  Supposons que les deux entiers a et b, on le même reste par la division euclidienne par r ; on en déduit :
  $$a-b=\left(q\cdot c+r\right)-\left(q'\cdot c+r\right)$$
  $$=\left(q\cdot c+r\right)-\left(q'\cdot c+r\right)=\left(q-q'\right)\cdot c$$
  On vient de montrer que $(a-b)$ est un multiple de c.

Proposition :

Deux entiers sont congrus entre eux modulo c si, et seulement, si leur différence est un multiple de c.

Démonstration :

La division euclidienne des entiers b et a permettent d'obtenir les couples $(q\,;r)$ et $\left(q'\,;r'\right)$ tels que :
$a=q\cdot c+r$ où $0\leqslant r\leqslant|c|$; $b=q'\cdot c+r'$ où $0\leqslant r'\leqslant|c|$

- $\Longrightarrow$:
  Supposons que le nombre $(a-b)$ est un multiple de c : il existe un entier k vérifiant :
  $a-b=k\cdot c$
  Le nombre $(a-b)$ peut s'écrire :
  $$a-b=\left(q-q'\right)\cdot c+\left(r-r'\right)$$
  $$k\cdot c=\left(q-q'\right)\cdot c+\left(r-r'\right)$$
  $$k\cdot c-\left(q-q'\right)\cdot c=\left(r-r'\right)$$
  $$r-r'=\left[k-\left(q-q'\right)\right]\cdot c$$
  On vient de montrer que le nombre $(r-r')$ est un multiple de c.

  Des propriétés des restes, on écrit :
  $$\left\{\begin{array}{l}0\leqslant r\leqslant|c|\\0\leqslant r'<|c|\end{array}\right.\Longrightarrow\left\{\begin{array}{r}0\leqslant r\leqslant|c|\\-|c|<r'\leqslant 0\end{array}\right.$$
  On en déduit l'encadrement suivant :
  $-|c|<r-r'<|c|$

  Dans l'intervalle $\left]-|c|\,;|c|\right[$, le seul multiple de c est 0 :
  $r-r'=0\quad\Longrightarrow\quad r=r'$

- $\Longleftarrow$:
  Supposons que les deux entiers a et b, on le même reste par la division euclidienne par r ; on en déduit :
  $$a-b=\left(q\cdot c+r\right)-\left(q'\cdot c+r\right)$$
  $$=\left(q\cdot c+r\right)-\left(q'\cdot c+r\right)=\left(q-q'\right)\cdot c$$
  On vient de montrer que $(a-b)$ est un multiple de c.

Proposition :

Deux entiers sont congrus entre eux modulo c si, et seulement, si leur différence est un multiple de c.

Démonstration :

La division euclidienne des entiers b et a permettent d'obtenir les couples $(q\,;r)$ et $\left(q'\,;r'\right)$ tels que :
$a=q\cdot c+r$ où $0\leqslant r\leqslant|c|$; $b=q'\cdot c+r'$ où $0\leqslant r'\leqslant|c|$

- $\Longrightarrow$:
  Supposons que le nombre $(a-b)$ est un multiple de c : il existe un entier k vérifiant :
  $a-b=k\cdot c$
  Le nombre $(a-b)$ peut s'écrire :
  $$a-b=\left(q-q'\right)\cdot c+\left(r-r'\right)$$
  $$k\cdot c=\left(q-q'\right)\cdot c+\left(r-r'\right)$$
  $$k\cdot c-\left(q-q'\right)\cdot c=\left(r-r'\right)$$
  $$r-r'=\left[k-\left(q-q'\right)\right]\cdot c$$
  On vient de montrer que le nombre $(r-r')$ est un multiple de c.

  Des propriétés des restes, on écrit :
  $$\left\{\begin{array}{l}0\leqslant r\leqslant|c|\\0\leqslant r'<|c|\end{array}\right.\Longrightarrow\left\{\begin{array}{r}0\leqslant r\leqslant|c|\\-|c|<r'\leqslant 0\end{array}\right.$$
  On en déduit l'encadrement suivant :
  $-|c|<r-r'<|c|$

  Dans l'intervalle $\left]-|c|\,;|c|\right[$, le seul multiple de c est 0 :
  $r-r'=0\quad\Longrightarrow\quad r=r'$

- $\Longleftarrow$:
  Supposons que les deux entiers a et b, on le même reste par la division euclidienne par r ; on en déduit :
  $$a-b=\left(q\cdot c+r\right)-\left(q'\cdot c+r\right)$$
  $$=\left(q\cdot c+r\right)-\left(q'\cdot c+r\right)=\left(q-q'\right)\cdot c$$
  On vient de montrer que $(a-b)$ est un multiple de c.