Congruence

Arithmétique et cryptographie

Sommaire

1. Relation de congruence.
2. Inverse multiplicatif.
3. Théorème des restes Chinois.

1. Relation de congruence.

1. Relation de congruence.

Concept de congruence

- La première formalisation de la notion de congruence date de 1801, avec la publication du Disquisitiones Arithmeticae de Gauss. Mais les idées sont beaucoup plus anciennes.

- En fait on ne va plus raisonner sur les nombres mais sur leurs restes dans la division euclidienne par un entier donné.

1. Relation de congruence.

Concept de congruence

- On a en effet constaté au chapitre précédent que les restes possibles après division euclidienne par un entier m étaient $0,1,2,\ldots,m-1$.

- C'est donc comme si l'on disposait de m boîtes, et que l'on mettait dans une même boîte les entiers ayant le même reste après division Euclidienne par m.

- Deux éléments d'une même boîte seront alors dits **congrus** modulo m.

1. Relation de congruence.

Concept de congruence : exemple

- Dans chacune des trois boîtes ci-dessous, les éléments sont congrus modulo 3 :

$\ldots,-9,-6,-3,0,3,6,9,\ldots$

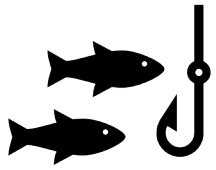
$\ldots,-8,-5,-2,1,4,7,10,\ldots$

$\ldots,-7,-4,-1,2,5,8,11,\ldots$

1. Relation de congruence.

Congruence : définition

- Soit m élément de $\mathbb{N}^*$.
- Deux entiers relatifs a et b sont dits **congrus modulo** m si et seulement si a et b possèdent le même reste après division Euclidienne par m.
- On note alors $a \equiv b\,[m]$.



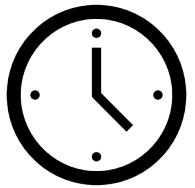
1. Relation de congruence.

Congruence : exemple

- On a $19 \equiv 43\,[12]$ car les restes de 19 et 43 après division Euclidienne par 12 valent tous deux 7.

- C'est pourquoi 7, 19 et 43 heures sont représentées par une même position des aiguilles sur un cadran de montre.

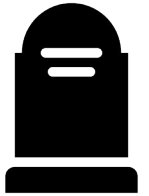
- D'ailleurs, la notion de congruence et les résultats qui en découlent sont aussi appelés arithmétique de l'horloge.



1. Relation de congruence.

Congruence : propriété élémentaire

- Soit m élément de $\mathbb{N}^*$, r élément de $\mathbb{N}$ et a élément de $\mathbb{Z}$.
- Si r est le reste de la division Euclidienne de a par m, alors $a \equiv r\,[m]$.
- Réciproquement si $0 \leq r < m$ et $a \equiv r\,[m]$ alors r est le reste de la division Euclidienne de a par m.

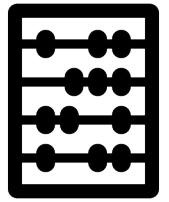


1. Relation de congruence.

Congruence : définition équivalente

- Soit m élément de $\mathbb{N}^*$.

- Deux entiers relatifs a et b sont dits **congrus modulo** m si et seulement si $a-b$ est un multiple de m.



1. Relation de congruence.

Congruence : propriétés des relations d'équivalence

- Soit m élément de $\mathbb{N}^*$.
- **Réflexivité** : pour tout entier relatif a, $a \equiv a\,[m]$.
- **Symétrie** : pour tous entiers relatifs a et b, $a \equiv b\,[m]$ est équivalent à $b \equiv a\,[m]$.
- **Transitivité** : pour tous entiers relatifs a, b et c, $a \equiv b\,[m]$ et $b \equiv c\,[m]$ impliquent $a \equiv c\,[m]$.

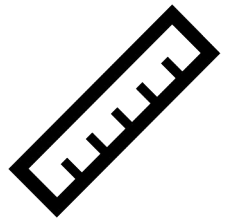
1. Relation de congruence.

Congruence : règles opératoires

- Soit m élément de $\mathbb{N}^*$ et a,b,c,d éléments de $\mathbb{Z}$.

- Si $a \equiv b\,[m]$ et $c \equiv d\,[m]$ alors

  1. $a + c \equiv b + d\,[m]$.
  2. $ac \equiv bd\,[m]$.
  3. Pour tout élément k de $\mathbb{N}^*$, $a^k \equiv b^k\,[m]$.



1. Relation de congruence.

Congruence : démonstration des règles opératoires

- D'après les hypothèses (et la définition équivalente des relations de congruence), il existe des entiers k et k' tels que $a = b + km$ et $c = d + k'm$.
- On a alors $a + c = b + d + (k + k')m$ ce qui prouve la première règle.
- On a aussi $ac = bd + (bk' + dk + kk'm)m$ ce qui prouve la deuxième règle.
- La troisième règle découle de la seconde par récurrence.

1. Relation de congruence.

Congruence : exemple d'application des règles opératoires

- Le reste de la division Euclidienne de 4^{2024} par 3 est égal à 1.

- En effet, $4 \equiv 1\,[3]$ donc d'après la troisième règle opératoire, $4^{2024} \equiv 1^{2024}\,[3]$.

- Et donc $4^{2024} \equiv 1\,[3]$.

1. Relation de congruence.

2. Inverse multiplicatif.

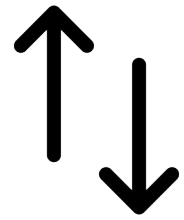
2. Inverse multiplicatif.

Inverse multiplicatif : définition

- Soit m élément de $\mathbb{N}^*$ et a élément de $\mathbb{Z}$.
- L'entier a est dit **inversible modulo** m s'il existe un entier relatif b tel que

$$ab \equiv 1\,[m]$$

- On dit alors que b est un **inverse multiplicatif** de a **modulo** m.



2. Inverse multiplicatif.

Inverse multiplicatif : remarques importantes

- Étant donné un entier m, tous les entiers ne sont pas nécessairement inversibles modulo m.

- Si un entier est inversible modulo m, son inverse n'est pas unique.

2. Inverse multiplicatif.

Inverse multiplicatif : exemples

- L'entier 5 est inversible modulo 7 et 3 est l'un de ses inverses multiplicatifs car $5 \times 3 \equiv 1\,[7]$.

- Comme autres inverses multiplicatifs de 5 modulo 7 on peut citer $10,17,-4,\ldots$

- Par contre 5 n'est pas inversible modulo 10. En effet, on vérifie facilement que pour tout entier b, on a soit $5b \equiv 0\,[10]$ soit $5b \equiv 5\,[10]$.

2. Inverse multiplicatif.

Inverse multiplicatif : remarque sur la notion d'inverse

- Ce concept d'inverse est formellement le même que celui des nombres réels.
- Rappelons en effet qu'un réel x est inversible dans $\mathbb{R}$ si et seulement si il existe un réel y tel que $xy = 1$.
- La seule différence étant les définitions des opérations et de l'élément unitaire.

2. Inverse multiplicatif.

Critère d'inversibilité : énoncé

- Soit m élément de $\mathbb{N}^*$ et a élément de $\mathbb{Z}$.

- L'entier a est inversible modulo m si et seulement si a est premier avec m, *i.e.* $\mathrm{PGCD}\,(a,m) = 1$.

2. Inverse multiplicatif.

Critère d'inversibilité : démonstration

- Si a est inversible modulo m, par définition il existe b tel que $ab \equiv 1\,[m]$. Cela signifie que $ab-1$ est un multiple de m et donc qu'il existe un entier k tel que $ab = 1 + km$. D'après le théorème de Bézout, a et m sont alors premiers entre eux.

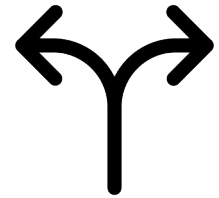
- Réciproquement, si a et m sont premiers entre eux, d'après ce même théorème de Bézout il existe des entiers u et v tels que $au + mv = 1$.
  On a alors $au \equiv 1\,[m]$, ce qui prouve bien que a est inversible modulo m.

2. Inverse multiplicatif.

Critère d'inversibilité : exemple

- L'entier 5 est inversible modulo 7 car $\mathrm{PGCD}\,(5,7) = 1.$

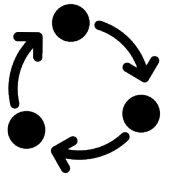
- Par contre 5 n'est pas inversible modulo 10 car $\mathrm{PGCD}\,(5,10) = 5.$



2. Inverse multiplicatif.

Méthode de calcul de l'inverse : principe

- Soit m élément de $\mathbb{N}^*$ et a élément de $\mathbb{Z}$.
- On suppose que l'entier a est inversible modulo m.
- Alors l'inverse multiplicatif de a modulo m est le coefficient de a dans sa relation de Bézout avec m.



2. Inverse multiplicatif.

Méthode de calcul de l'inverse : exemple

- Vérifions que 9 est inversible modulo 26 et calculons son inverse.

- On utilise tout d'abord l'algorithme d'Euclide pour prouver que $\mathrm{PGCD}\,(9{,}26) = 1$, et pour calculer les coefficients de Bézout de 9 et 26

$$3 \times 9 + (-1) \times 26 = 1$$

- Le fait que 9 et 26 soient premiers entre eux implique que 9 est inversible modulo 26 et la relation de Bézout nous donne son inverse, à savoir 3.

2. Inverse multiplicatif.

3. Théorème des restes Chinois.

3. Théorème des restes Chinois.

Contexte historique

- On trouve trace du théorème suivant, dit théorème chinois, dans des écrits du 1er siècle : le Jiuzhang suanshu (prescriptions de calcul en neuf chapitres).

- Il permet la résolution de problèmes du type :

  - On a un certain nombre d'objets tel que si on les compte par 3 il en reste 2, si on les compte par 5 il en reste 3 et si on les compte par 7 il en reste 2; combien y a-t-il d'objets ?

3. Théorème des restes Chinois.

Théorème des restes chinois : énoncé

- On considère le système

$$\begin{cases} x \equiv a_1\,[m_1] \\ x \equiv a_2\,[m_2] \\ \vdots \\ x \equiv a_n\,[m_n] \end{cases}$$

- Où $m_1,m_2,\ldots,m_n$ sont des éléments de $\mathbb{N}^*$ premiers entre eux deux à deux, et $a_1,a_2,\ldots,a_n$ des éléments de $\mathbb{N}$ tels que

$$0 \leq a_1 < m_1, 0 \leq a_2 < m_2, \ldots, 0 \leq a_n < m_n$$

3. Théorème des restes Chinois.

Théorème des restes chinois : énoncé

- Soit

$$M = m_1 \times m_2 \times \ldots \times m_n$$

- Le système précédent admet une unique solution modulo M donnée par

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n$$

- Où

$$M_i = \frac{M}{m_i} \quad et \quad y_i M_i \equiv 1 \, [m_i]$$

3. Théorème des restes Chinois.

Théorème des restes chinois : démonstration

- On montre d'abord que pour tout i tel que $1 \leq i \leq n$, $PGCD\,(M_i,m_i) = 1$. On a

$$M_i = \frac{M}{m_i} = m_1 \times \ldots \times m_{i-1} \times m_{i+1} \times \ldots \times m_n$$

- D'après le théorème d'Euclide (voir prochain chapitre du cours), un diviseur premier commun à m_i et M_i diviserait nécessairement un des m_j pour un $j \neq i$.

- Mais cela contredirait le fait que $PGCD\left(m_i,m_j\right) = 1$. Il n'en existe donc pas et par suite $PGCD\,(M_i,m_i) = 1$.

3. Théorème des restes Chinois.

Théorème des restes chinois : démonstration

- D’après le critère d’inversibilité de la partie précédente cela prouve que M_i est inversible modulo m_i, et donc qu'il existe un entier y_i tel que $M_i y_i \equiv 1\,[m_i]$.
- On peut donc bien définir x tel que cela est fait dans l’énoncé du théorème.
- Pour montrer que x est bien solution du système, il faut vérifier que $x \equiv a_j\,[m_j]$ pour tout j tel que $1 \leq j \leq n$.

3. Théorème des restes Chinois.

Théorème des restes chinois : démonstration

- Puisque
$$M_i = m_1 \times \ldots \times m_{i-1} \times m_{i+1} \times \ldots \times m_n$$
- Il est clair que $M_i \equiv 0 \left[m_j\right]$ pour tout $i \neq j$. Par suite $x \equiv a_j M_j y_j \left[m_j\right]$.
- Or comme on l'a vu précédemment $M_j y_j \equiv 1 \left[m_j\right]$, donc $x \equiv a_j \left[m_j\right]$.
- Cela étant vrai pour tous les j on en déduit que x est bien une solution du système.

3. Théorème des restes Chinois.

Théorème des restes chinois : démonstration

- Il reste à prouver l'unicité modulo M. Pour cela considérons x' une autre solution du système et montrons que $x \equiv x' \,[M]$.
- Comme $x \equiv a_j \,[m_j]$ et $x' \equiv a_j \,[m_j]$, on a $x \equiv x' \,[m_j]$ pour tout j, $1 \leq j \leq n$.
- Cela signifie que pour tout j, $m_j | \,(x - x')$.
- Puisque les m_j sont premiers entre eux deux à deux, le corollaire du théorème de Gauss (cf. chapitre précédent) implique que $M | \,(x - x')$, et donc que $x \equiv x' \,[M]$. Q.E.D.

3. Théorème des restes Chinois.