

Fiche A1.4 : Applications des congruences

1 - Critères de divisibilité

- Tout entier naturel N s'écrit en base 10 : $N = a_p 10^p + a_{p-1} 10^{p-1} + \dots + a_1 10 + a_0$, où $a_0, a_1, \dots, a_p$ sont ses chiffres (entre 0 et 9) ; a_0 est le chiffre des unités.

Propriété 1 : Soit N un entier naturel de chiffres $a_p, \dots, a_1, a_0$.

- $N \equiv a_0 \pmod{10}$: N est divisible par 2 (resp. 5) si et seulement si son chiffre des unités l'est.
- $N \equiv a_0 + a_1 + \dots + a_p \pmod{9}$: N est divisible par 9 (resp. 3) si et seulement si la somme de ses chiffres l'est.
- $N \equiv 10a_1 + a_0 \pmod{4}$: N est divisible par 4 si et seulement si le nombre formé par ses 2 derniers chiffres l'est.
- $N \equiv a_0 - a_1 + a_2 - \dots + (-1)^p a_p \pmod{11}$: N est divisible par 11 si et seulement si la somme alternée de ses chiffres l'est.

Démonstration : on applique la compatibilité des congruences (fiche A1.3) à l'écriture de N en base 10.

- $10^k \equiv 0 \pmod{10}$ pour $k \geq 1$, donc $N \equiv a_0 \pmod{10}$. Même raisonnement modulo 2 et 5.
- $10 \equiv 1 \pmod{9}$, donc $10^k \equiv 1 \pmod{9}$ pour tout k , et $N \equiv a_p + \dots + a_1 + a_0 \pmod{9}$. Même raisonnement modulo 3.
- $100 \equiv 0 \pmod{4}$, donc $10^k \equiv 0 \pmod{4}$ pour $k \geq 2$, et $N \equiv 10a_1 + a_0 \pmod{4}$.
- Enfin $10 \equiv -1 \pmod{11}$, donc $10^k \equiv (-1)^k \pmod{11}$ et $N \equiv a_0 - a_1 + a_2 - \dots \pmod{11}$. $\square$

Exemple 1 : Le nombre $N = 7392816$ est-il divisible par 3 ? par 9 ? par 4 ? par 11 ?

- $7 + 3 + 9 + 2 + 8 + 1 + 6 = 36$ est divisible par 9 : N est divisible par 9, donc par 3.
- 16 est divisible par 4 : N aussi.
- En partant des unités : $6 - 1 + 8 - 2 + 9 - 3 + 7 = 24 \equiv 2 \pmod{11}$: N n'est pas divisible par 11 (le reste est 2).

Exemple 2 : Déterminer les chiffres x tels que le nombre $\overline{3x52}$ (écrit en base 10) soit divisible par 3.

$\overline{3x52} \equiv 3 + x + 5 + 2 = 10 + x \pmod{3}$. Il est divisible par 3 si et seulement si $x \equiv -10 \equiv 2 \pmod{3}$, soit $x \in \{2 ; 5 ; 8\}$.

2 - Résoudre des équations avec des congruences

- On rappelle qu'on a pas le droit de diviser une égalité de congruence par un même nombre. Pour résoudre une équation, on dispose alors de deux méthodes pour résoudre

Méthode 1 (table de congruences) : modulo n , un entier x n'a que n restes possibles. On teste, pour chaque reste de x , le reste de l'expression étudiée.

Exemple 3 : Résoudre dans $\mathbb{Z}$ l'équation $3x \equiv 5 \pmod{7}$.

Reste de x modulo 7	0	1	2	3	4	5	6
Reste de $3x$ modulo 7	0	3	6	2	5	1	4

$3x \equiv 5 \pmod{7} \Leftrightarrow x \equiv 4 \pmod{7}$: les solutions sont les entiers $x = 4 + 7k$, avec $k \in \mathbb{Z}$.

Exemple 4 : Démontrer que l'équation $x^2 = 3y + 2$ n'a aucune solution $(x ; y)$ dans $\mathbb{Z}^2$.

Si $(x ; y)$ est solution, alors $x^2 \equiv 2 \pmod{3}$. Or modulo 3 : si $x \equiv 0$, $x^2 \equiv 0$; si $x \equiv 1$, $x^2 \equiv 1$; si $x \equiv 2$, $x^2 \equiv 4 \equiv 1$.

Un carré n'est donc jamais congru à 2 modulo 3 : l'équation n'a pas de solution entière.

Définition : Soit $n \geq 2$. On dit que $a \in \mathbb{Z}$ admet un **inverse modulo** n s'il existe un entier u tel que $au \equiv 1 [n]$.

Exemple 5 : Trouver un inverse du nombre 3 modulo [11] : $3 \times 4 \equiv 12 \equiv 1 [11]$ Donc 4 est un inverse de 3.

Remarque : tout entier n'a pas d'inverse : $2u$ est pair, donc $2u \equiv 1[4]$ est impossible. Au chapitre suivant, on verra que a a un inverse modulo n si et seulement si a et n sont premiers entre eux.

Méthode 2 (inverse) : On cherche d'abord un inverse du nombre qui est situé devant le « x ».

Puis on multiplie les deux membres de l'équation par cet inverse trouvé.

Exemple 6 : Résoudre dans $\mathbb{Z}$ l'équation $3x - 9 \equiv 4 [11]$.

$$3x - 9 \equiv 4 [11] \Leftrightarrow 3x \equiv 4 + 9 \equiv 13[11] \Leftrightarrow 3x \equiv 2[11] \Leftrightarrow 4 \times 3x \equiv 4 \times 2[11] \Leftrightarrow x \equiv 8[11]$$

3 - Clés de contrôle

• Pour détecter les erreurs de saisie, on ajoute à un code une **clé** calculée avec des congruences : codes-barres, ISBN, RIB, numéro de sécurité sociale...

Exemple 7 : (code EAN-13) : un code-barres de 13 chiffres $a_1 a_2 \dots a_{13}$ est valide si $a_1 + 3a_2 + a_3 + 3a_4 + \dots + 3a_{12} + a_{13} \equiv 0 [10]$.

a) Déterminer la clé a_{13} du code 978221005432 a_{13} .

$$9 + 3 \times 7 + 8 + 3 \times 2 + 2 + 3 \times 1 + 0 + 3 \times 0 + 5 + 3 \times 4 + 3 + 3 \times 2 = 75.$$

Il faut $75 + a_{13} \equiv 0 [10]$, d'où $a_{13} = 5$.

b) Montrer qu'une erreur sur un seul chiffre est toujours détectée.

Si un chiffre a de coefficient $c \in \{1 ; 3\}$ est remplacé par $a' \neq a$, la somme varie de $c(a' - a)$ avec $0 < |a' - a| \leq 9$.

Si $c = 1$, $a' - a \not\equiv 0 [10]$. Si $c = 3$: $3(a' - a) \equiv 0 [10]$ et $-27 \leq 3(a' - a) \leq 27$ entraînerait $3(a' - a) \in \{\pm 10; \pm 20\}$ ce qui est impossible car aucun d'entre eux n'est multiple de 3.

L'erreur est donc toujours détectée pour une erreur sur un seul chiffre (mais pas forcément sur plusieurs).

4 - Chiffrement affine

• On numérote les lettres de $A = 0$ à $Z = 25$. Le **chiffrement affine** de clé $(a ; b)$ remplace la lettre de numéro x par la lettre de numéro y , où y est le reste de $ax + b$ modulo 26.

Exemple 8 : On choisit la clé $(3 ; 7)$.

a) Chiffrer le mot MATHS.

- | | | |
|--|---|--|
| • M : $3 \times 12 + 7 = 43 \equiv 17 \rightarrow R$; | • A : $7 \rightarrow H$; | • T : $3 \times 19 + 7 = 64 \equiv 12 \rightarrow M$; |
| • H : $3 \times 7 + 7 = 28 \equiv 2 \rightarrow C$; | • S : $3 \times 18 + 7 = 61 \equiv 9 \rightarrow J$. | • Le mot chiffré est RHM CJ. |

b) Exprimer x en fonction de y et déchiffrer la lettre R.

$3 \times 9 = 27 \equiv 1[26]$ Donc 9 est un inverse de 3 modulo 26 et on va donc pour voir résoudre l'équation :

$$y \equiv 3x + 7 [26] \Leftrightarrow 3x \equiv y - 7 [26] \Leftrightarrow 9 \times 3x \equiv 9(y - 7) [26] \Leftrightarrow x \equiv 9(y - 7) = 9y - 63 [26],$$

soit $x \equiv 9y + 15 [26]$ car $-63 + 78 = 15$.

Pour R ($y = 17$) : $9 \times 17 + 15 = 168 \equiv 12 [26]$: c'est bien M.

Remarque : avec la clé $(2 ; 0)$, les lettres x et $x + 13$ sont chiffrées de la même façon ($2 \times 13 = 26 \equiv 0 [26]$) : on ne peut pas déchiffrer. Il faut que a ait un inverse modulo 26.