Vous avez dit (In)congrus 2017-2018

IREM de Limoges

Faculté des Sciences & Techniques

Plan

Points communs ?

Mathématiques indispensables dans la HauteTechnologie : codes détecteurs d'erreurs, codes correcteurs d'erreurs, cryptographie

Plan

Divisibilité dans $\mathbb{N}$

- Soient a et b deux entiers naturels. On dit que a **divise** b s'il existe entier naturel q tel que $b = aq$.

Divisibilité dans $\mathbb{N}$

- Soient a et b deux entiers naturels. On dit que a **divise** b s'il existe entier naturel q tel que $b = aq$.
- On dit aussi que a est un diviseur de b ou que b est un multiple de a ou encore b est divisible par a.

Divisibilité dans $\mathbb{N}$

- Soient a et b deux entiers naturels. On dit que a **divise** b s'il existe entier naturel q tel que $b = aq$.
- On dit aussi que a est un diviseur de b ou que b est un multiple de a ou encore b est divisible par a.
- **Exemples**

Divisibilité dans $\mathbb{N}$

- Soient a et b deux entiers naturels. On dit que a **divise** b s'il existe entier naturel q tel que $b = aq$.
- On dit aussi que a est un diviseur de b ou que b est un multiple de a ou encore b est divisible par a.
- **Exemples**
  - L'entier naturel 3 divise 9 mais 3 ne divise pas 17.

Divisibilité dans $\mathbb{N}$

- Soient a et b deux entiers naturels. On dit que a **divise** b s'il existe entier naturel q tel que $b = aq$.
- On dit aussi que a est un diviseur de b ou que b est un multiple de a ou encore b est divisible par a.
- **Exemples**
  - L'entier naturel 3 divise 9 mais 3 ne divise pas 17.
  - Tout entier naturel divise 0 et l'entier 1 divise tout entier naturel.

Divisibilité dans $\mathbb{Z}$

- Soient a et b deux entiers relatifs. On dit que a **divise** b s'il existe entier relatif q tel que $b = aq$.

Divisibilité dans $\mathbb{Z}$

- Soient a et b deux entiers relatifs. On dit que a **divise** b s'il existe entier relatif q tel que $b = aq$.
- On dit aussi que a est un diviseur de b ou que b est un multiple de a ou encore b est divisible par a.

Divisibilité dans $\mathbb{Z}$

- Soient a et b deux entiers relatifs. On dit que a **divise** b s'il existe entier relatif q tel que $b = aq$.
- On dit aussi que a est un diviseur de b ou que b est un multiple de a ou encore b est divisible par a.
- **Exemples**

Divisibilité dans $\mathbb{Z}$

- Soient a et b deux entiers relatifs. On dit que a **divise** b s'il existe entier relatif q tel que $b = aq$.
- On dit aussi que a est un diviseur de b ou que b est un multiple de a ou encore b est divisible par a.
- **Exemples**
  - L'entier relatif -3 divise 9 mais -3 ne divise pas 17.

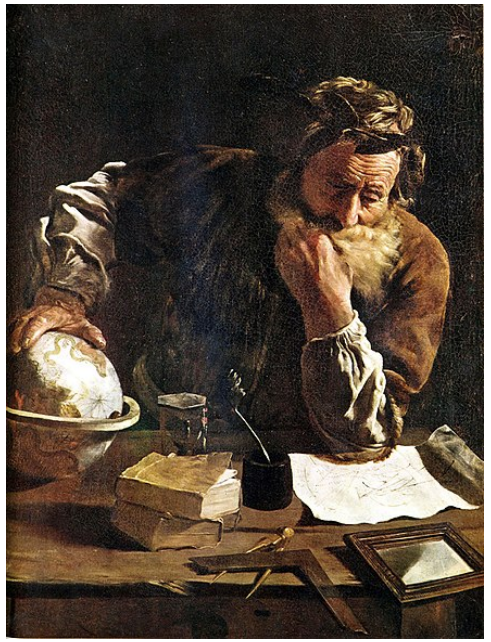
Divisibilité dans $\mathbb{Z}$

- Soient a et b deux entiers relatifs. On dit que a **divise** b s'il existe entier relatif q tel que $b = aq$.
- On dit aussi que a est un diviseur de b ou que b est un multiple de a ou encore b est divisible par a.
- **Exemples**
  - L'entier relatif -3 divise 9 mais -3 ne divise pas 17.
  - Tout nombre relatif divise 0 et l'entier -1 divise tout entier naturel.

Lemme d'Archimède

Soit a un entier naturel et b un entier naturel non nul. Alors il existe un multiple de b strictement plus grand que a .

Si a est la longueur _____ et b ___ ,
Alors $4b$ est la longueur _____
et $5b$ est la longueur _____



Vers 262 av. J.-C. —- Vers 190 av. J.-C.

Division dans $\mathbb{Z}$

Théorème
Quels que soient les entiers relatifs a et b (avec $b \neq 0$), il existe un unique couple (q, r) d'entiers relatifs tel que

$$a = bq + r \text{ et } 0 \leq r \leq |b|.$$

Définitions

- L'entier a est le dividende

Vers 325 av. J.-C. –Vers 265 av. J.-C.

Division dans $\mathbb{Z}$

Théorème
Quels que soient les entiers relatifs a et b (avec $b \neq 0$), il existe un unique couple (q, r) d'entiers relatifs tel que

$$a = bq + r \text{ et } 0 \leq r \leq |b|.$$

Définitions

- L'entier a est le dividende
- L'entier b est le diviseur

Vers 325 av. J.-C. –Vers 265 av. J.-C.

Division dans $\mathbb{Z}$

Théorème
Quels que soient les entiers relatifs a et b (avec $b \neq 0$), il existe un unique couple (q, r) d'entiers relatifs tel que

$$a = bq + r \text{ et } 0 \leq r \leq |b|.$$

Définitions

- L'entier a est le dividende
- L'entier b est le diviseur
- L'entier q est le quotient

Vers 325 av. J.-C. –Vers 265 av. J.-C.

Division dans $\mathbb{Z}$

Théorème
Quels que soient les entiers relatifs a et b (avec $b \neq 0$), il existe un unique couple (q, r) d'entiers relatifs tel que

$$a = bq + r \text{ et } 0 \leq r \leq |b|.$$

Définitions

- L'entier a est le dividende
- L'entier b est le diviseur
- L'entier q est le quotient
- L'entier r est le reste

Vers 325 av. J.-C. –Vers 265 av. J.-C.

Plan

Congruences

30 avril 1777 - 23 Février 1855

Congruences

Définition

Soit n un entier naturel non nul et soient a et b deux entiers relatifs. On dit que a est congru à b modulo n si n divise $a - b$

- **Notation** $a \equiv b \pmod{n}$

Congruences

Définition

Soit n un entier naturel non nul et soient a et b deux entiers relatifs. On dit que a est congru à b modulo n si n divise $a - b$

- **Notation** $a \equiv b \pmod{n}$
- **Exemples**

Congruences

Définition

Soit n un entier naturel non nul et soient a et b deux entiers relatifs. On dit que a est congru à b modulo n si n divise $a - b$

- **Notation** $a \equiv b \pmod{n}$
- **Exemples**
  - On a : $9 \equiv 29 \pmod{10}$.

Congruences

Définition

Soit n un entier naturel non nul et soient a et b deux entiers relatifs. On dit que a est congru à b modulo n si n divise $a - b$

- **Notation** $a \equiv b \pmod{n}$
- **Exemples**
  - On a : $9 \equiv 29 \pmod{10}$.
  - De même : $109 \equiv 9 \equiv -1 \pmod{10}$.
  - Mais 7 n'est pas congru à 35 modulo 10.

Congruences

Propriétés Soit n un entier naturel non nul.

- La relation être congru à modulo n est une relation d'équivalence.

Congruences

Propriétés Soit n un entier naturel non nul.

- La relation être congru à modulo n est une relation d'équivalence.
- Soient a et b deux entiers relatifs. On a : a est congru à b modulo n si et seulement si a et b ont même reste dans la division par n.

Congruences

Propriétés Soit n un entier naturel non nul.

- La relation être congru à modulo n est une relation d'équivalence.
- Soient a et b deux entiers relatifs. On a : a est congru à b modulo n si et seulement si a et b ont même reste dans la division par n.
- Tout nombre relatif est congru modulo n à un et un seul nombre entre 0 et $n-1$: son reste dans la division par n.

Congruences

Propriétés Soit n un entier naturel non nul.

- La relation être congru à modulo n est une relation d'équivalence.
- Soient a et b deux entiers relatifs. On a : a est congru à b modulo n si et seulement si a et b ont même reste dans la division par n.
- Tout nombre relatif est congru modulo n à un et un seul nombre entre 0 et $n-1$: son reste dans la division par n.
- **Exemple** $204 \equiv 201 \equiv 0 \pmod 3$

Travailler modulo n

On travaille comme dans l'ensemble $\mathbb{Z}$ mais en tenant compte que $n \equiv 0 \pmod{n}$ et donc tout multiple de n est congru à 0 modulo n.

Exemple
Soit $A = 100 \times 5 + 22$. Calculons rapidement le reste de A dans la division euclidienne par 3 (sans effectuer cette dernière).
On a :

Travailler modulo n

On travaille comme dans l'ensemble $\mathbb{Z}$ mais en tenant compte que $n \equiv 0 \pmod{n}$ et donc tout multiple de n est congru à 0 modulo n.

Exemple
Soit $A = 100 \times 5 + 22$. Calculons rapidement le reste de A dans la division euclidienne par 3 (sans effectuer cette dernière).
On a :
$100 \equiv 1 \pmod{3}$, $5 \equiv 2 \pmod{3}$ et $22 \equiv 1 \pmod{3}$.

Travailler modulo n

On travaille comme dans l'ensemble $\mathbb{Z}$ mais en tenant compte que $n \equiv 0 \pmod{n}$ et donc tout multiple de n est congru à 0 modulo n.

Exemple
Soit $A = 100 \times 5 + 22$. Calculons rapidement le reste de A dans la division euclidienne par 3 (sans effectuer cette dernière).
On a :
$100 \equiv 1 \pmod{3}$, $5 \equiv 2 \pmod{3}$ et $22 \equiv 1 \pmod{3}$.
Donc $A \equiv$

Travailler modulo n

On travaille comme dans l'ensemble $\mathbb{Z}$ mais en tenant compte que $n \equiv 0 \pmod{n}$ et donc tout multiple de n est congru à 0 modulo n.

Exemple
Soit $A = 100 \times 5 + 22$. Calculons rapidement le reste de A dans la division euclidienne par 3 (sans effectuer cette dernière).
On a :
$100 \equiv 1 \pmod{3}$, $5 \equiv 2 \pmod{3}$ et $22 \equiv 1 \pmod{3}$.
Donc $A \equiv 1 \times$

Travailler modulo n

On travaille comme dans l'ensemble $\mathbb{Z}$ mais en tenant compte que $n \equiv 0 \pmod{n}$ et donc tout multiple de n est congru à 0 modulo n.

Exemple
Soit $A = 100 \times 5 + 22$. Calculons rapidement le reste de A dans la division euclidienne par 3 (sans effectuer cette dernière).
On a :
$100 \equiv 1 \pmod{3}$, $5 \equiv 2 \pmod{3}$ et $22 \equiv 1 \pmod{3}$.
Donc $A \equiv 1 \times 5 +$

Travailler modulo n

On travaille comme dans l'ensemble $\mathbb{Z}$ mais en tenant compte que $n \equiv 0 \pmod{n}$ et donc tout multiple de n est congru à 0 modulo n.

Exemple

Soit $A = 100 \times 5 + 22$. Calculons rapidement le reste de A dans la division euclidienne par 3 (sans effectuer cette dernière).

On a :

$100 \equiv 1 \pmod{3}$, $5 \equiv 2 \pmod{3}$ et $22 \equiv 1 \pmod{3}$.

Donc $A \equiv 1 \times 5 + 1$

Travailler modulo n

On travaille comme dans l'ensemble $\mathbb{Z}$ mais en tenant compte que $n \equiv 0 \pmod{n}$ et donc tout multiple de n est congru à 0 modulo n.

Exemple
Soit $A = 100 \times 5 + 22$. Calculons rapidement le reste de A dans la division euclidienne par 3 (sans effectuer cette dernière).
On a :
$100 \equiv 1 \pmod{3}$, $5 \equiv 2 \pmod{3}$ et $22 \equiv 1 \pmod{3}$.
Donc $A \equiv 1 \times 5 + 1 \equiv 0 \pmod{3}$.

Plan

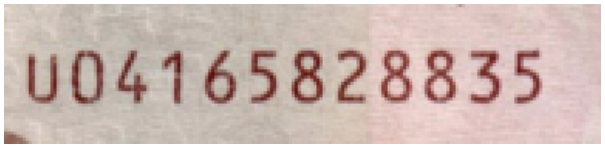
Billets

Billet de 10 euros.

Billets

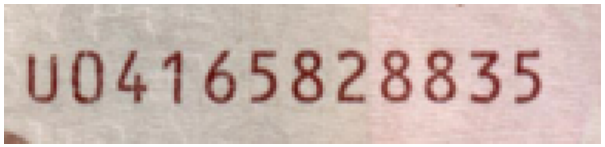
Allemagne	X	88
Autriche	N	78
Belgique	Z	90
Espagne	V	86
Finlande	L	76
France	U	85
Grèce	Y	89
Irlande	T	84
Italie	S	83
Luxembourg	R	82
Pays-Bas	P	80
Portugal	M	77

Billets



- On remplace la lettre U par son code ASCII ici 85

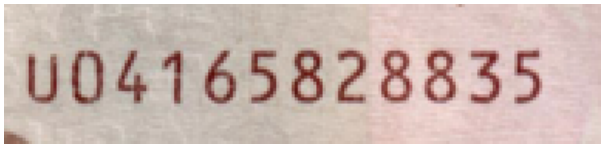
Billets



- On remplace la lettre U par son code ASCII ici 85
- Le nombre $N = 8504165828835$ obtenu

doit être congru à 0 modulo 9.

Billets



- On remplace la lettre U par son code ASCII ici 85
- Le nombre $N = 8504165828835$ obtenu

> *doit être congru à 0 modulo* 9.

- $8+5+0+4+1+6+5+8+2+8+8+3+5 = 63$

Travailler modulo n

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Travailler modulo 4

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Critères de divisibilité

- Par 2,5,3,9,10

Critères de divisibilité

- Par 2,5,3,9,10
- Par 11 : $\overline{ABCDEFG} \equiv 0 \pmod{11}$ si et seulement si $G - F + E - D + C - B + A \equiv 0 \pmod{11}$.
  Exemple
  L'entier naturel 3014 est-il divisible par 11 ?

Plan

Règle de luhn

$$N = \begin{array}{cccccccccc} 7 & 3 & 2 & 8 & 2 & 9 & 3 & 2 & 0 \end{array}$$

Règle de luhn

$$N = \begin{array}{ccccccccc} 7 & 3 & 2 & 8 & 2 & 9 & 3 & 2 & 0 \end{array}$$
$$N = \begin{array}{ccccccccc} \boxed{7} & 3 & \boxed{2} & 8 & \boxed{2} & 9 & \boxed{3} & 2 & \boxed{0} \end{array}$$

Règle de luhn

$$N = 7\ 3\ 2\ 8\ 2\ 9\ 3\ 2\ 0$$
$$N = \boxed{7}\ 3\ \boxed{2}\ 8\ \boxed{2}\ 9\ \boxed{3}\ 2\ \boxed{0}$$

$\boxed{7}\ \boxed{2}\ \boxed{2}\ \boxed{3}\ \boxed{0}$ ____ Somme ____ $\boxed{7}+\boxed{2}+\boxed{2}+\boxed{3}+\boxed{0}=14$

Règle de luhn

$$N = 7\ 3\ 2\ 8\ 2\ 9\ 3\ 2\ 0$$
$$N = \boxed{7}\ 3\ \boxed{2}\ 8\ \boxed{2}\ 9\ \boxed{3}\ 2\ \boxed{0}$$

$\boxed{7}\ \boxed{2}\ \boxed{2}\ \boxed{3}\ \boxed{0}$ ____ Somme ____ $\boxed{7}+\boxed{2}+\boxed{2}+\boxed{3}+\boxed{0}=14$

$\square\,3\,\square\,8\,\square\,9\,\square\,2\,\square$

Règle de luhn

$N = 7\ 3\ 2\ 8\ 2\ 9\ 3\ 2\ 0$

$N = \boxed{7}\ 3\ \boxed{2}\ 8\ \boxed{2}\ 9\ \boxed{3}\ 2\ \boxed{0}$

$\boxed{7}\ \boxed{2}\ \boxed{2}\ \boxed{3}\ \boxed{0}$ ____ Somme ____ $\boxed{7}+\boxed{2}+\boxed{2}+\boxed{3}+\boxed{0}=14$

$\square\ 3\ \square\ 8\ \square\ 9\ \square\ 2\ \square$ _____ $\times 2$ _____ $6\ \ 16\ \ 18\ \ 4$

_

Règle de luhn

$$N = 7\ 3\ 2\ 8\ 2\ 9\ 3\ 2\ 0$$
$$N = \boxed{7}\ 3\ \boxed{2}\ 8\ \boxed{2}\ 9\ \boxed{3}\ 2\ \boxed{0}$$

$\boxed{7}\ \boxed{2}\ \boxed{2}\ \boxed{3}\ \boxed{0}$ ___ Somme ___ $\boxed{7}+\boxed{2}+\boxed{2}+\boxed{3}+\boxed{0}=14$

$\square\,3\,\square\,8\,\square\,9\,\square\,2\,\square$ _____ $\times 2$ _____ $6\ \ 16\ \ 18\ \ 4$

_ Somme de chiffres _ $6+7+9+4$

Règle de luhn

$$N = 7\ 3\ 2\ 8\ 2\ 9\ 3\ 2\ 0$$
$$N = \boxed{7}\ 3\ \boxed{2}\ 8\ \boxed{2}\ 9\ \boxed{3}\ 2\ \boxed{0}$$

$\boxed{7}\ \boxed{2}\ \boxed{2}\ \boxed{3}\ \boxed{0}$ ___ Somme ___ $\boxed{7}+\boxed{2}+\boxed{2}+\boxed{3}+\boxed{0}=14$

$\square\,3\,\square\,8\,\square\,9\,\square\,2\,\square$ _____ $\times 2$ _____ $6\ \ 16\ \ 18\ \ 4$

_ Somme de chiffres _ $6+7+9+4=26$

Règle de luhn

$$N = 7\ 3\ 2\ 8\ 2\ 9\ 3\ 2\ 0$$
$$N = \boxed{7}\ 3\ \boxed{2}\ 8\ \boxed{2}\ 9\ \boxed{3}\ 2\ \boxed{0}$$

$\boxed{7}\ \boxed{2}\ \boxed{2}\ \boxed{3}\ \boxed{0}$ ___ Somme ___ $\boxed{7}+\boxed{2}+\boxed{2}+\boxed{3}+\boxed{0}=14$

$\square\,3\,\square\,8\,\square\,9\,\square\,2\,\square$ _____ $\times 2$ _____ $6\ \ 16\ \ 18\ \ 4$

_ Somme de chiffres _ $6+7+9+4=26$

$+ = 40 \equiv 0\ [10]$

Règle de Luhn

- Vérification facile de la clé : on teste si $L(N) \equiv 0\ [10]$

Règle de Luhn

- Vérification facile de la clé : on teste si $L(N) \equiv 0\ [10]$
- Construction de la clé soit D nombre à 8 chiffres on cherche $cl \in \{0,1,2,3,4,5,6,7,8,9\}$ tel que $L(10D + cl) \equiv 0 \pmod{10}$

Règle de Luhn

- Vérification facile de la clé : on teste si $L(N) \equiv 0\ [10]$
- Construction de la clé soit D nombre à 8 chiffres on cherche $cl \in \{0,1,2,3,4,5,6,7,8,9\}$ tel que $L(10D + cl) \equiv 0 \pmod{10}$

Règle de Luhn

- Vérification facile de la clé : on teste si $L(N) \equiv 0$ [10]
- Construction de la clé soit D nombre à 8 chiffres on cherche $cl \in \{0,1,2,3,4,5,6,7,8,9\}$ tel que $L(10D + cl) \equiv 0 \pmod{10}$

On a $L(10D + cl) = L(10D) + cl$ et donc $cl \equiv -L(10D)$ [10].

Règle de Luhn

- Vérification facile de la clé : on teste si $L(N) \equiv 0$ [10]
- Construction de la clé soit D nombre à 8 chiffres on cherche $cl \in \{0,1,2,3,4,5,6,7,8,9\}$ tel que $L(10D + cl) \equiv 0 \pmod{10}$

On a $L(10D + cl) = L(10D) + cl$ et donc $cl \equiv -L(10D)$ [10].
Si r est le chiffre des unités de $L(10D)$,
$cl = 10 - r$ et si $r = 0$ alors $cl = 0$.

Règle de luhn

$$D = \begin{array}{cccccccc} 5 & 1 & 2 & 8 & 2 & 9 & 3 & 3 \end{array}$$

Règle de luhn

$$\begin{array}{rccccccccccccccc} D = & & 5 & & 1 & & 2 & & 8 & & 2 & & 9 & & 3 & & 3 \\ 10D = & \boxed{5} & & 1 & & \boxed{2} & & 8 & & \boxed{2} & & 9 & & \boxed{3} & & 3 & & \boxed{0} \end{array}$$

Règle de luhn

$$D = 5\ 1\ 2\ 8\ 2\ 9\ 3\ 3$$
$$10D = \boxed{5}\ 1\ \boxed{2}\ 8\ \boxed{2}\ 9\ \boxed{3}\ 3\ \boxed{0}$$

$$\boxed{5}\ \boxed{2}\ \boxed{2}\ \boxed{3}\ \boxed{0} \quad \text{Somme} \quad \boxed{5}+\boxed{2}+\boxed{2}+\boxed{3}+\boxed{0}=12$$

Règle de luhn

$$D = 5\ 1\ 2\ 8\ 2\ 9\ 3\ 3$$

$$10D = \boxed{5}\ 1\ \boxed{2}\ 8\ \boxed{2}\ 9\ \boxed{3}\ 3\ \boxed{0}$$

$\boxed{5}\ \boxed{2}\ \boxed{2}\ \boxed{3}\ \boxed{0}$ ___ Somme ___ $\boxed{5}+\boxed{2}+\boxed{2}+\boxed{3}+\boxed{0}=12$

$\square\ 1\ \square\ 8\ \square\ 9\ \square\ 3\ \square$

Règle de luhn

$$D = \ 5 \quad 1 \quad 2 \quad 8 \quad 2 \quad 9 \quad 3 \quad 3$$

$$10D = \boxed{5} \quad 1 \quad \boxed{2} \quad 8 \quad \boxed{2} \quad 9 \quad \boxed{3} \quad 3 \quad \boxed{0}$$

$\boxed{5} \quad \boxed{2} \quad \boxed{2} \quad \boxed{3} \quad \boxed{0}$ ____ Somme ____ $\boxed{5}+\boxed{2}+\boxed{2}+\boxed{3}+\boxed{0}=12$

$\square\,1\,\square\,8\,\square\,9\,\square\,3\,\square$ _____ $\times 2$ _____ 2 16 18 6

_ Somme de chiffres _ $2+7+9+6$

Règle de luhn

$$D = \ 5 \quad 1 \quad 2 \quad 8 \quad 2 \quad 9 \quad 3 \quad 3$$
$$10D = \boxed{5} \quad 1 \quad \boxed{2} \quad 8 \quad \boxed{2} \quad 9 \quad \boxed{3} \quad 3 \quad \boxed{0}$$

$\boxed{5} \quad \boxed{2} \quad \boxed{2} \quad \boxed{3} \quad \boxed{0}$ ___ Somme ___ $\boxed{5}+\boxed{2}+\boxed{2}+\boxed{3}+\boxed{0}=12$

$\square\,1\,\square\,8\,\square\,9\,\square\,3\,\square$ _____ $\times 2$ _____ $2 \quad 16 \quad 18 \quad 6$

_ Somme de chiffres _ $2+7+9+6=24$

Règle de luhn

$$D = \begin{array}{cccccccccc} 5 & 1 & 2 & 8 & 2 & 9 & 3 & 3 \end{array}$$

$$10D = \begin{array}{cccccccccc} \boxed{5} & 1 & \boxed{2} & 8 & \boxed{2} & 9 & \boxed{3} & 3 & \boxed{0} \end{array}$$

$\boxed{5}\ \boxed{2}\ \boxed{2}\ \boxed{3}\ \boxed{0}$ ___ Somme ___ $\boxed{5}+\boxed{2}+\boxed{2}+\boxed{3}+\boxed{0}=12$

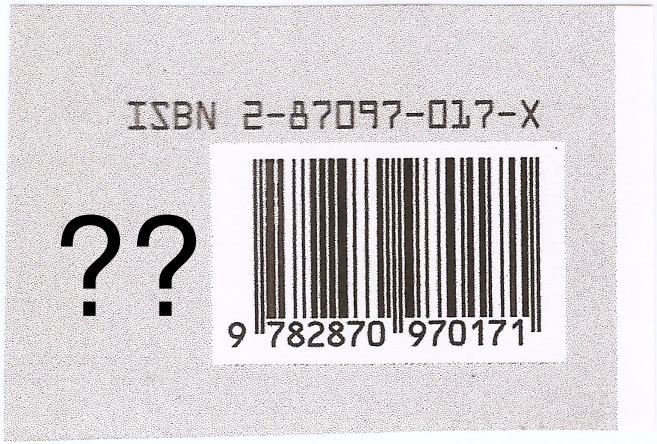
$\square\,1\,\square\,8\,\square\,9\,\square\,3\,\square$ _____ $\times 2$ _____ $2\quad 16\quad 18\quad 6$

_ Somme de chiffres _ $2+7+9+6=24$

$+ = 36 \equiv 6 \pmod{10}$

et donc la clé vaut 4.

Plan



À vous de jouer pendant les ateliers...

Merci de votre attention et profitez bien des ateliers !!