

ARITHMÉTIQUE

Activité 1 : Motivation.

- a) Trouver un entier naturel divisible par 2 et 3 qui est aussi divisible par 6.
Trouver si possible un entier naturel divisible par 2 et 3 et qui n'est pas divisible par 6.
- b) Trouver un entier naturel divisible par 4 et 10 qui est aussi divisible par 40.
Trouver si possible un entier naturel divisible par 4 et 10 et qui n'est pas divisible par 40.

Synthèse :

Un nombre (12; 30; ...) qui est à la fois divisible par 2 et 3 est divisible par 6.

Par contre, un nombre (20; 60 ; etc) divisible par 4 et 10 n'est pas nécessairement divisible par 40.

Dans ce chapitre, nous justifierons ces deux situations qui peuvent nous paraître paradoxales.

Notions préliminaires :

- Addition et multiplication dans $\mathbb{N}$:

L'ensemble des nombres entiers naturels est noté $\mathbb{N}$. On a :

$\mathbb{N} = \{0 ; 1 ; 2 ; 3 ; \dots\}$ et $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Propriétés 1 :

Pour tous entiers naturels a , b et c , on a :

P1) $a + b \in \mathbb{N}$ (+ dans $\mathbb{N}$ est une loi de composition interne)

P2) $a + 0 = 0 + a = a$. (0 est élément neutre pour +.)

P3) $a + (b + c) = (a + b) + c$ (+ est associative.)

P4) $a + b = b + a$ (+ est commutative.)

P5) $a + c = b + c \Rightarrow a = b$

P6) $a + b = 0 \Rightarrow a = b = 0$

Propriétés 2 :

P1) $a \times b \in \mathbb{Z}$ ($\times$ dans $\mathbb{N}$ est une loi de composition interne)

P2) $a \times 1 = 1 \times a = a$ (1 est élément neutre pour $\times$.)

P3) $a \times (b \times c) = (a \times b) \times c$ ($\times$ est associative.)

P4) $a \times b = b \times a$ ($\times$ est commutative.)

P5) $a \times (b + c) = a \times b + a \times c$ ($\times$ est distributive par rapport à +)

P6) $a \times c = b \times c \Rightarrow a = b$ avec $c \in \mathbb{N}^*$.

$$P7) \quad a \times b = 1 \Rightarrow a = b = 1$$

• **Relation d'ordre sur $\mathbb{N}$:**

On définit dans $\mathbb{N}$ une relation, notée $\leq$, par :

$$\forall (a; b) \in \mathbb{N}^2, a \leq b \Leftrightarrow \exists c \in \mathbb{N}, b = a + c.$$

Propriétés 1 :

Pour tous entiers naturels a, b et c , on a :

$$P1) \quad a \leq a \quad (\text{la relation } \leq \text{ est réflexive})$$

$$P2) \quad \text{si } a \leq b \text{ et } b \leq a, \text{ alors } a = b \quad (\text{la relation } \leq \text{ est antisymétrique})$$

$$P3) \quad \text{si } a \leq b \text{ et } b \leq c, \text{ alors } a \leq c \quad (\text{la relation } \leq \text{ est transitive})$$

On dit que $\leq$ dans $\mathbb{N}$ est une relation d'ordre.

Deux entiers naturels a et b sont toujours comparables, c'est-à-dire on a toujours :

$a \leq b$ ou $b \leq a$; on dit que $\leq$ dans $\mathbb{N}$ est une relation d'ordre total.

Activité :

a) Résoudre dans $\mathbb{N}^2$ l'équation : $x(y-3)=1$.

b) Résoudre dans $\mathbb{N}^2$ le système suivant :

$$\begin{cases} xy \leq 2x \\ x + y = 4 \end{cases}$$

Solution :

a) Résolution dans $\mathbb{N}^2$ de l'équation : $x(y-3)=1$.

$$\forall (x; y) \in \mathbb{N}^2, x(y-3)=1 \Leftrightarrow \begin{cases} x=1 \\ y-3=1 \end{cases} \Leftrightarrow \begin{cases} x=1 \\ y=4 \end{cases}$$

$$S = \{(1; 4)\}$$

b) Résolution dans $\mathbb{N}^2$ du système : $\begin{cases} xy \leq 2x \\ x + y = 4 \end{cases}$.

Première méthode :

$$\begin{aligned} \forall (x; y) \in \mathbb{N}^2, xy \leq 2x &\Leftrightarrow xy - 2x \leq 0 \\ &\Leftrightarrow x(y-2) \leq 0 \\ &\Leftrightarrow x=0 \text{ ou } y-2 \leq 0 \\ &\Leftrightarrow x=0 \text{ ou } y \in [0; 2] \end{aligned}$$

• Si $x=0$, alors $x+y=4 \Rightarrow y=4$.

• Si $y=0$, alors $x+y=4 \Rightarrow x=4$.

• Si $y=1$, alors $x+y=4 \Rightarrow x=3$.

• Si $y=2$, alors $x+y=4 \Rightarrow x=2$.

$$S = \{(0; 4); (4; 0); (3; 1); (2; 2)\}$$

Deuxième méthode :

$$\forall (x; y) \in \mathbb{N}^2, x+y=4 \Leftrightarrow (x; y) \in \{(0;4);(4;0);(1;3);(3;1);(2;2)\}.$$

En remplaçant x et y par leurs valeurs dans l'inéquation : $xy \leq 2x$, on a :

- pour $(x; y)=(0;4)$, $xy \leq 2x \Rightarrow 0 \leq 0$ Inégalité vraie
 - pour $(x; y)=(4;0)$, $xy \leq 2x \Rightarrow 0 \leq 8$ Inégalité vraie
 - pour $(x; y)=(1;3)$, $xy \leq 2x \Rightarrow 3 \leq 2$ Inégalité fausse
 - pour $(x; y)=(3;1)$, $xy \leq 2x \Rightarrow 3 \leq 6$ Inégalité vraie
 - pour $(x; y)=(2;2)$, $xy \leq 2x \Rightarrow 4 \leq 4$ Inégalité vraie
- d'où $S = \{(0;4);(4;0);(3;1);(2;2)\}$.

• Raisonnement par récurrence :

Soit n et n_0 deux entiers naturels et $P(n)$ une proposition dépendant de n .

Pour démontrer qu'une proposition $P(n)$ est vraie pour tout n supérieur ou égal à n_0 , on peut procéder comme suit :

- ◆ Vérifier que $P(n_0)$ est vraie ;
- ◆ Supposer que $P(n)$ est vraie pour tout $n \geq n_0$ et montrer que $P(n+1)$ est vraie.

Exemple :

Soit $P(n)$ la propriété « Pour tout entier naturel n non nul, on a :

$$\sum_{k=1}^n k(k+1) = \frac{n(n+1)(n+2)}{3} \quad \gg$$

$$P(1) \text{ est vraie car } \sum_{k=1}^1 k(k+1) = \frac{(1)(1+1)(1+2)}{3}.$$

$$\text{En effet, } \sum_{k=1}^1 k(k+1) = (1)(1+1) = 2 \text{ et } \frac{(1)(1+1)(1+2)}{3} = \frac{6}{3} = 2$$

Supposons que $P(n)$ est vraie, c'est-à-dire « Pour tout entier naturel n non nul, on a :

$$\sum_{k=1}^n k(k+1) = \frac{n(n+1)(n+2)}{3} \gg, \text{ et montrons que } P(n+1) \text{ est vraie,}$$

$$\text{c'est-à-dire } \sum_{k=1}^{n+1} k(k+1) = \frac{(n+1)(n+2)(n+3)}{3}.$$

$$\text{On a : } \sum_{k=1}^{n+1} k(k+1) = \left[\sum_{k=1}^n k(k+1) \right] + (n+1)(n+2)$$

$$= \frac{n(n+1)(n+2)}{3} + (n+1)(n+2) \quad \text{d'après l'hypothèse}$$

$$= \frac{n(n+1)(n+2) + 3(n+1)(n+2)}{3}$$

$$\sum_{k=1}^{n+1} k(k+1) = \frac{(n+1)(n+2)(n+3)}{3} \quad \text{CQFD}$$

$$\text{Conclusion : } \forall n \in \mathbb{N}^*, \sum_{k=1}^n k(k+1) = \frac{n(n+1)(n+2)}{3}.$$

Activité :

Démontrer que pour tout entier naturel n , $3^{2n+1} + 2^{n+2}$ est divisible par 7.

Solution :

Soit $P(n)$ la propriété : « Pour tout entier naturel n , $3^{2n+1} + 2^{n+2}$ est divisible par 7. ».

On a : $P(0)$: « $3^{2(0)+1} + 2^{0+2} = 3 + 4 = 7$ est divisible par 7. » est vraie.

Supposons que la propriété est vraie à l'ordre n et montrons qu'elle l'est à l'ordre $n+1$.

$$\text{On a : } \forall n \in \mathbb{N}, 3^{2(n+1)+1} + 2^{(n+1)+2} = 3^{2n+2+1} + 2^{n+1+2}$$

$$= 3^{2n+1}(3^2) + 2^{n+2}(2)$$

$$= 3^{2n+1}(9) + 2^{n+2}(2)$$

$$= 3^{2n+1}(7+2) + 2^{n+2}(2)$$

$$= 3^{2n+1}(7) + 3^{2n+1}(2) + 2^{n+2} \times 2$$

$$= 3^{2n+1}(7) + 2(3^{2n+1} + 2^{n+2})$$

$\forall n \in \mathbb{N}, 3^{2n+1}(7)$ est divisible par 7 et d'après l'hypothèse, $3^{2n+1} + 2^{n+2}$ est divisible par 7 d'où $3^{2n+1}(7) + 2(3^{2n+1} + 2^{n+2})$ est divisible par 7.

Donc $P(n+1)$ est vraie.

• Addition et multiplication dans $\mathbb{Z}$:

L'ensemble des entiers relatifs est noté $\mathbb{Z}$. On a :

$\mathbb{Z} = \{ \dots ; -3 ; -2 ; -1 ; 0 ; 1 ; 2 ; 3 ; \dots \}$ et $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

Propriétés 1 : Addition

Pour tous entiers relatifs a , b et c , on a :

- P1) $a+b \in \mathbb{Z}$ (+ dans $\mathbb{Z}$ est une loi de composition interne)
- P2) $a+0=0+a=a$. (0 est élément neutre pour +.)
- P3) $a+(b+c)=(a+b)+c$ (+ est associative.)
- P4) $\exists a' \in \mathbb{Z}, a+a'=a'+a=0$ (tout élément x de $\mathbb{Z}$ a un opposé $-x$ dans $\mathbb{Z}$)
- P5) $a+b=b+a$ (+ est commutative.)
- P6) $a+c=b+c \Rightarrow a=b$ (tout élément de $\mathbb{Z}$ est régulier pour +)

Remarque :

Pour résumer les 4 premières propriétés, on dit que $(\mathbb{Z}, +)$ est un groupe.

On dit que $(\mathbb{Z}, +)$ est un groupe commutatif pour résumer les 5 premières propriétés.

Propriétés 2 : Multiplication

Pour tous entiers relatifs a, b et c , on a :

- P1) $a \times b \in \mathbb{Z}$ ($\times$ dans $\mathbb{Z}$ est une loi de composition interne)
- P2) $a \times (b \times c) = (a \times b) \times c$ ($\times$ est associative.)
- P3) $a \times (b+c) = a \times b + a \times c$ ($\times$ est distributive par rapport à +)
- P4) $a \times b = b \times a$ ($\times$ est commutative.)
- P5) $a \times 1 = 1 \times a = a$ (1 est élément neutre pour $\times$.)
- P6) $a \times c = b \times c \Rightarrow a = b$ avec $c \in \mathbb{Z}^*$.
- P7) $a \times b = 1 \Rightarrow a = b = 1$ ou $a = b = -1$.

Remarques :

- Pour résumer les 5 premières propriétés susmentionnées de l'addition et de la multiplication, on dit que $(\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire.
- D'une manière générale, soit $(A, +, \times)$ un anneau commutatif unitaire non nul, c'est-à-dire qu'il possède au moins deux éléments.

On dit que $(A, +, \times)$ est un anneau intègre si et seulement si :

$$\forall (a; b) \in A^2, a \times b = 0 \Rightarrow a = 0 \text{ ou } b = 0.$$

• **Relation d'ordre sur $\mathbb{Z}$:**

On définit sur $\mathbb{Z}$ la relation, notée $\leq$, par :

$$\forall (a ; b) \in \mathbb{Z}^2, a \leq b \Leftrightarrow b - a \in \mathbb{N}.$$

1. **Systèmes de numération :**

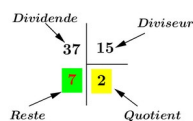
1.1. **Division euclidienne dans $\mathbb{N}$:**

Activité :

On donne $a=37$ et $b=15$.

- Déterminer deux entiers naturels q et r tels que $a=bq+r$.
- Comment appelle-t-on a, b, q et r .

Solution :



On a : $q=2$ et $r=7$.

Théorème :

Quels que soient le nombre entier naturel a et le nombre entier naturel non nul b , il existe un unique couple $(q;r)$ de nombres entiers naturels tel que :

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

q et r sont appelés respectivement quotient et reste de la division euclidienne de a par b .

1.2. Écriture d'un nombre dans une base donnée :

Soit b un entier naturel supérieur ou égal à 2.

Tout entier naturel x non nul peut s'écrire de façon unique

$$\sum_{k=0}^p a_k b^k = a_p b^p + a_{p-1} b^{p-1} + \dots + a_2 b^2 + a_1 b + a_0, \text{ où les } a_k \text{ sont des entiers}$$

naturels tels que : $0 \leq a_k < b$ et $a_p \neq 0$.

On écrit : $x = \overline{a_p a_{p-1} \dots a_2 a_1 a_0}^b$. Cette écriture est appelée écriture de x en base b .

Par convention, les écritures sans « barre » sont en base 10.

Les principales bases sont :

- Le système décimal : base 10

Les dix symboles (chiffres) utilisés dans le système décimal sont : 0 ; 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 ; 9.

C'est le système qui est couramment utilisé.

$$\text{En effet, } 25784 = 2 \times 10^4 + 5 \times 10^3 + 7 \times 10^2 + 8 \times 10 + 4$$

- Le système binaire : base 2

La numération binaire est surtout utilisée pour décrire le fonctionnement des machines électroniques (calculatrices, ordinateurs, ...).

Les chiffres utilisés sont 0 et 1.

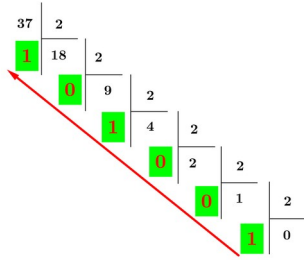
Exemples :

Écrivons $\overline{101101}^2$ dans le système décimal

$$\overline{101101}^2 = 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 0 \times 2 + 1 = 32 + 8 + 4 + 1 = 45$$

Écrivons 37 dans le système binaire.

Pour cela, on effectue des divisions successives par 2 comme indiqué ci-dessous jusqu'à ce que le quotient soit nul.



$$37 = \overline{100101}^2$$

- **Le système hexadécimal** : base 16

Les symboles utilisés dans le système hexadécimal sont :

0 ; 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 ; 9 ; A ; B ; C ; D ; E ; F.

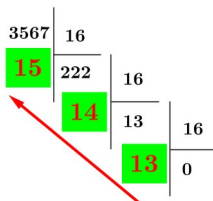
Les lettres A ; B ; C ; D ; E ; F représentent respectivement dans le système décimal les nombres 10 ; 11 ; 12 ; 13 ; 14 ; 15.

Exemples :

Écrivons dans le système décimal $\overline{BAC}^{16}$:

$$\overline{BAC}^{16} = 11(16^2) + 10(16) + 12 = 2816 + 160 + 12 = 2988$$

Écrivons 3567 dans le système hexadécimal :



$$3567 = \overline{DEF}^{16}$$

Activité :

b est un entier naturel strictement supérieur à 1.

Écrire $(b+1)^2$ en base b . (On distinguera deux cas : $b=2$ et $b \neq 2$.)

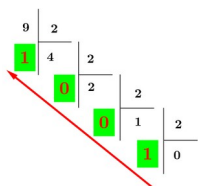
Solution :

Premier cas : $b=2$.

$$(b+1)^2 = 3^2 = 9.$$

En remarquant que $9 = 8 + 1 = 2^3 + 1$, on a : $9 = \overline{1001}^2$.

On peut également faire des divisions successives par 2.



d'où $9 = \overline{1001}^2$.

Deuxième cas : $b \neq 2 \Rightarrow b \geq 3$.

On a : $(b+1)^2 = b^2 + 2b + 1 = (1)b^2 + (2)b + (1)b^0$.

$b > 1$ et $b > 2$ d'où $(b+1)^2 = \overline{121}^b$.

2. Congruence modulo n :

2.1. Division euclidienne dans $\mathbb{Z}$:

Soit a et b deux entiers relatifs tels que $b \neq 0$.

Il existe un unique couple $(q ; r)$ de $\mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < |b|$.

q est appelé le quotient et r le reste de la division euclidienne de a par b .

Activité :

Effectuer la division euclidienne de a par b dans chacun des cas suivants :

- a) $a = 35$ et $b = 13$
- b) $a = -35$ et $b = 13$
- c) $a = 35$ et $b = -13$
- d) $a = -35$ et $b = -13$
- e) $a = 13$ et $b = 35$
- f) $a = -13$ et $b = -35$

Solution :

- a) $a = 35$ et $b = 13$

$$\begin{array}{r|l} 35 & 13 \\ 9 & 2 \end{array}$$

On a : $35 = 13(2) + 9$

- b) $a = -35$ et $b = 13$

$$\begin{aligned} 35 = 13(2) + 9 &\Leftrightarrow -35 = -13(2) - 9 \\ &\Leftrightarrow -35 = 13(-2) - 9 \\ &\Leftrightarrow -35 = 13(-2) - 13 + 13 - 9 \\ &\Leftrightarrow -35 = 13(-2-1) + 4 \\ &\Leftrightarrow -35 = 13(-3) + 4 \end{aligned}$$

- c) $a = 35$ et $b = -13$

$$35 = 13(2) + 9 \Leftrightarrow 35 = -13(-2) + 9$$

- d) $a = -35$ et $b = -13$

$$\begin{aligned} 35 = 13(2) + 9 &\Leftrightarrow -35 = -13(2) - 9 \\ &\Leftrightarrow -35 = -13(2) - 13 + 13 - 9 \\ &\Leftrightarrow -35 = -13(2+1) + 4 \\ &\Leftrightarrow -35 = -13(3) + 4 \end{aligned}$$

NB : Ce résultat peut être déduit de b).

En effet, $-35 = 13(-3) + 4 \Leftrightarrow -35 = -13(3) + 4$.

e) $a=13$ et $b=35$

$$\begin{array}{r|l} 13 & 35 \\ 13 & 0 \end{array}$$

$$13=35(0)+13$$

f) $a=-13$ et $b=-35$

$$\begin{aligned} 13 &= 35(0) + 13 \Leftrightarrow -13 = -35(0) - 13 \\ &\Leftrightarrow -13 = -35(0) - 35 + 35 - 13 \\ &\Leftrightarrow -13 = -35(1) + 22 \end{aligned}$$

2.2. Multiples et diviseurs d'un entier relatif :

Soit a et b deux entiers relatifs.

On dit que a est un multiple de b s'il existe un entier relatif k tel que $a=kb$.

Si de plus $b \neq 0$, on dit que b est un diviseur de a ou que b divise a .

La relation " b divise a " est notée b/a .

Exemples :

On a : $14=2 \times 7$. On dit que 14 est un multiple de 2 et de 7 ou encore que 2 et 7 divisent 14.

De même, -2 et -3 sont des diviseurs de 6.

Remarques :

- 1 et -1 divisent tout entier relatif.
- Tout entier relatif non nul divise 0, mais 0 ne divise aucun entier relatif.
- Un entier relatif non nul b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

Propriétés 1 : $\forall (a;b;c) \in (\mathbb{Z}^*)^3$

P1) a/a

P2) $\begin{cases} a/b \\ b/c \end{cases} \Rightarrow a/c$

P3) $\begin{cases} a/b \\ b/a \end{cases} \Rightarrow a=b \text{ ou } a=-b$

P4) $\begin{cases} a/b \\ a/c \end{cases} \Rightarrow a/(pb+qc) \text{ avec } (p;q) \in \mathbb{Z}^2$

L'ensemble des multiples d'un entier relatif b est noté $b\mathbb{Z}$.

On a :

- $2\mathbb{Z} = \{ \dots; -4; -2; 0; 2; 4; 6; 8; \dots \}$.
- $2\mathbb{Z} = -2\mathbb{Z}$; $1\mathbb{Z} = \mathbb{Z}$ et $0\mathbb{Z} = \{0\}$.

L'ensemble des diviseurs d'un entier relatif a est souvent noté $D(a)$ ou $\text{Div}(a)$.

On a :

- $D(12) = \{ -12; -6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 12 \}$

- $D(-12)=D(12)$; $D(1)=[-1;1]$ et $D(0)=\mathbb{Z}^*$.

Remarques : Soit a un entier relatif.

- Si x est un diviseur de a , alors $-x$ est un diviseur de a
- 1 et a sont des diviseurs de a .
- Si x_1 et x_2 sont deux entiers relatifs tels que $a=x_1 \times x_2$, alors $x_1 \leq \sqrt{|a|}$ ou $x_2 \leq \sqrt{|a|}$.
- Des remarques précédentes, on peut déduire des diviseurs de a compris entre 2 et $\sqrt{|a|}$, l'ensemble des diviseurs de a .

Exemple : Déterminons l'ensemble des diviseurs de 56.

$$\sqrt{56} \simeq 7,48.$$

On a : $56=2 \times 28$; 3 ne divise pas 56; $56=4 \times 14$; 5 et 6 ne divisent pas 56; $56=7 \times 8$ d'où l'ensemble des diviseurs de 56 est :

$$D(56)=[-56 ; -28 ; -14 ; -8 ; -7 ; -4 ; -2 ; -1 ; 1 ; 2 ; 4 ; 7 ; 8 ; 14 ; 28 ; 56]$$

Activité :

Résoudre dans $(\mathbb{N}^*)^2$ l'équation : $a^2 - b^2 = 196$.

Solution :

$$\forall (a;b) \in (\mathbb{N}^*)^2, a^2 - b^2 = 196 \Leftrightarrow (a-b)(a+b) = 196 \Rightarrow \begin{cases} a-b < 0 \\ a+b < 0 \end{cases} \text{ ou } \begin{cases} a-b > 0 \\ a+b > 0 \end{cases}$$

Or $\forall (a;b) \in (\mathbb{N}^*)^2, a+b > 0$ et $a-b < a+b$ d'où $0 < a-b < a+b$.

$$\sqrt{196} = 14$$

$$\text{On a : } (a-b)(a+b) = 196 = 1 \times 196 = 2 \times 98 = 4 \times 49 = 7 \times 28 = 14 \times 14$$

$$\text{Donc } \begin{cases} a-b=1 \\ a+b=196 \end{cases} \text{ ou } \begin{cases} a-b=2 \\ a+b=98 \end{cases} \text{ ou } \begin{cases} a-b=4 \\ a+b=49 \end{cases} \text{ ou } \begin{cases} a-b=7 \\ a+b=28 \end{cases}$$

Or $\forall (a;b) \in (\mathbb{N}^*)^2, a-b$ et $a+b$ ont la même parité d'où

$$\begin{cases} a-b=2 \\ a+b=98 \end{cases} \Leftrightarrow \begin{cases} 2a=100 \\ 2b=96 \end{cases} \Leftrightarrow \begin{cases} a=50 \\ b=48 \end{cases}$$

2.3. Nombres premiers :

Définition 1 : On dit qu'un entier naturel p est premier s'il possède exactement deux diviseurs positifs : 1 et p .

Définition 2 : Un nombre entier naturel n est dit premier s'il n'admet seulement que deux diviseurs positifs distincts : 1 et n .

Un entier naturel est dit *composé* lorsqu'il n'est pas premier.

Exemples :

2; 7 et 19 sont des nombres premiers.

4 et 35 ne sont pas des nombres premiers.

Remarques :

- 0 n'est pas premier car il possède une infinité de diviseurs.
- 1 n'est pas premier car il ne possède qu'un seul diviseur positif.
- Il existe une infinité de nombres premiers.

L'ensemble des entiers naturels premiers inférieurs ou égaux à 100 est :

$\{2; 3; 5; 7; 11; 13; 17; 19; 23; 29; 31; 37; 41; 43; 47; 53; 59; 61; 67; 71; 73; 79; 83; 89; 97\}$

.

Propriété :

Soit n un entier naturel strictement supérieur à 1.

Si n n'admet pas de diviseur premier p tel que $p \leq \sqrt{n}$, alors n est un nombre premier.

Exemples : Vérifions si 283 et 371 sont des nombres premiers.

- On a : $\sqrt{283} \approx 16,82$.

Il s'agit donc de vérifier si 283 est divisible par 2; 3; 5; 7; 11 ou 13.

$$283 = 2 \times 141 + 1$$

$$283 = 3 \times 94 + 1$$

$$283 = 5 \times 56 + 3$$

$$283 = 7 \times 40 + 3$$

$$283 = 11 \times 25 + 8$$

$$283 = 13 \times 21 + 10$$

283 est un nombre premier car aucun des nombres premiers inférieurs ou égaux à $\sqrt{283}$ ne divise 283.

- On a : $\sqrt{371} \approx 19,26$

Vérifions si 371 est divisible par 2; 3; 5; 7; 11; 13; 17 ou 19.

$$371 = 2 \times 185 + 1$$

$$371 = 3 \times 123 + 2$$

$$371 = 5 \times 74 + 1$$

$$371 = 7 \times 53$$

371 est divisible par 7. Donc il n'est pas premier.

Propriété :

Tout entier naturel $n \in \mathbb{N} \setminus \{0; 1\}$ peut s'écrire comme un produit de nombres premiers : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$ où p_i sont des nombres premiers et $\alpha_i \in \mathbb{N}$ avec $i \in \{1; 2; \dots; k\}$.

Cette décomposition en facteurs premiers est unique à l'ordre des facteurs près.

Le nombre de diviseurs positifs de n est : $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$.

Exemple : Décomposons 756 en produit de facteurs premiers.

756	2
378	2
189	3
63	3
21	3
7	7
1	

$$756 = 2^2 \times 3^3 \times 7$$

2.4. Congruence modulo n avec $n \in \mathbb{N}^*$:

Soit n un entier naturel non nul, a et b deux entiers relatifs.

On dit que a est congru à b modulo n si $a-b$ est un multiple de n .

On écrit : $a \equiv b[n]$.

Exemples : $53 \equiv 3 [5]$; $-41 \equiv 1 [3]$; $3 \equiv -2 [5]$; $100 \equiv 0 [10]$.

Remarques :

Si r désigne le reste de la division euclidienne de a par n , alors $a \equiv r[n]$.

Propriétés :

Soit n et k deux entiers naturels non nuls, a, b, c et d quatre entiers relatifs.

- P1) $a \equiv a[n]$ (on dit que la relation de congruence modulo n est réflexive)
- P2) Si $a \equiv b[n]$, alors $b \equiv a[n]$ (on dit que la relation de congruence modulo n est symétrique)
- P3) $\begin{cases} a \equiv b[n] \\ b \equiv c[n] \end{cases} \Rightarrow a \equiv c[n]$ (on dit que la relation de congruence modulo n est transitive)
- P4) $\begin{cases} a \equiv b[n] \\ c \equiv d[n] \end{cases} \Rightarrow a+c \equiv b+d[n]$
- P5) $\begin{cases} a \equiv b[n] \\ c \equiv d[n] \end{cases} \Rightarrow ac \equiv bd[n]$
- P6) $a \equiv b[n] \Rightarrow a^k \equiv b^k[n]$

Pour résumer les trois premières propriétés, on dit que la relation de congruence modulo n est une relation d'équivalence.

Activité :

A. On donne $a=235$ et $b=87$.

- Déterminer, en utilisant la congruence, les restes des divisions euclidiennes de a et b par 7.
- En déduire les restes des divisions euclidiennes de $2a-5b$ et $-a^3+4b^2$ par 7.

B. Déterminer suivant les valeurs de l'entier naturel n , le reste de la division euclidienne de 11^n par 7.

En déduire le reste de la division euclidienne de 11^{2015} par 7.

C. Soit x un entier naturel non nul et $\overline{a_p a_{p-1} \dots a_2 a_1 a_0}$ son écriture décimale.

On a donc : $x = a_p 10^p + a_{p-1} 10^{p-1} + \dots + a_2 10^2 + a_1 \times 10 + a_0$.

Démontrer que :

- $x \equiv a_0[2]$

- b) $x \equiv a_0[5]$
 c) $x \equiv \overline{a_1 a_0}[4]$
 d) $x \equiv a_p + a_{p-1} + \dots + a_2 + a_1 + a_0[3]$
 e) $x \equiv a_p + a_{p-1} + \dots + a_2 + a_1 + a_0[9]$
 f) $x \equiv a_p(-1)^p + a_{p-1}(-1)^{p-1} + \dots + a_2(-1)^2 + a_1(-1) + a_0[11]$

En déduire les restes des divisions euclidiennes de 2357 par 2; par 3; par 4; par 5 et par 11.

Solution :

A. On a : $a=235$ et $b=87$.

a) Les restes des divisions de a et b par 7.

On a : $235 \equiv 4[7]$ et $87 \equiv 3[7]$.

4 et 3 sont des entiers naturels strictement inférieurs à 7.

Donc les restes des divisions de a et b par 7 sont respectivement 4 et 3.

b) Les restes des divisions euclidiennes de $2a-5b$ et $-a^3+4b^2$ par 7.

• On a : $a \equiv 4[7]$ et $b \equiv 3[7]$.

Donc $(2a-5b) \equiv (2 \times 4 - 5 \times 3)[7] \Leftrightarrow (2a-5b) \equiv -7[7] \Leftrightarrow (2a-5b) \equiv 0[7]$ d'où le reste de la division euclidienne de $2a-5b$ par 7 est 0.

• On a : $a \equiv 4[7]$ et $b \equiv 3[7]$.

Donc $-a^3+4b^2 \equiv -(4^3)+4(3^2)[7] \Leftrightarrow -a^3+4b^2 \equiv -64+36[7]$
 $\Leftrightarrow -a^3+4b^2 \equiv -28[7]$
 $\Leftrightarrow -a^3+4b^2 \equiv 0[7]$

d'où le reste de la division euclidienne de $-a^3+4b^2$ par 7 est 0.

B. Le reste de la division euclidienne de 11^n par 7.

On a : $11^0 \equiv 1[7]$

$11^1 \equiv 4[7]$

$11^2 \equiv 2[7]$

$11^3 \equiv 1[7]$

Donc $\forall k \in \mathbb{N}$, on a : $11^{3k} \equiv 1[7]$; $11^{3k+1} \equiv 4[7]$; $11^{3k+2} \equiv 2[7]$.

Le reste de la division euclidienne de 11^n par 7 est :

- 1 si $n=3k$;
- 4 si $n=3k+1$;
- 2 si $n=3k+2$.

On a : $11^{2015} = 11^{671(3)+2} \equiv 2[7]$.

d'où le reste de la division euclidienne de 11^{2015} par 7 est 2.

C. On a : $x = a_p 10^p + a_{p-1} 10^{p-1} + \dots + a_2 10^2 + a_1 \times 10 + a_0$.

a) Divisibilité par 2 :

On a : $10 \equiv 0[2]$ d'où $a_p 10^p + a_{p-1} 10^{p-1} + \dots + a_2 10^2 + a_1 \times 10 \equiv 0[2]$.

Donc $x \equiv a_0[2]$.

Conséquence : Un nombre est divisible par 2 si son dernier chiffre est congru à zéro modulo 2. Par exemple, 2357 n'est pas divisible par 2 car son dernier chiffre 7 n'est pas divisible par 2.

b) Divisibilité par 5 :

On a : $10 \equiv 0[5]$ d'où $a_p 10^p + a_{p-1} 10^{p-1} + \dots + a_2 10^2 + a_1 \times 10 \equiv 0[5]$.

Donc $x \equiv a_0[5]$.

Conséquence : Un nombre est divisible par 5 si son dernier chiffre est congru à zéro modulo 5.

2357 n'est pas divisible par 5 car son dernier chiffre 7 n'est pas divisible par 5.

c) Divisibilité par 4 :

On a : $10^2 \equiv 0[4]$ d'où $a_p 10^p + a_{p-1} 10^{p-1} + \dots + a_2 10^2 \equiv 0[4]$.

Donc $x \equiv \overline{a_1 a_0}[4]$.

Conséquence : Un nombre est divisible par 4 si le nombre formé par ses deux derniers chiffres est congru à zéro modulo 4.

2357 n'est pas divisible par 4 car 57 n'est pas divisible par 4.

d) Divisibilité par 3 :

On a : $10 \equiv 1[3]$ d'où $x \equiv a_p + a_{p-1} + \dots + a_2 + a_1 + a_0[3]$.

Conséquence : Un nombre est divisible par 3 si la somme de ses chiffres est congru à zéro modulo 3.

e) Divisibilité par 9 :

On a : $10 \equiv 1[9]$ d'où $x \equiv a_p + a_{p-1} + \dots + a_2 + a_1 + a_0[9]$.

Conséquence : Un nombre est divisible par 9 si la somme de ses chiffres est congru à zéro modulo 9.

f) Divisibilité par 11 :

On a : $10 \equiv -1[11]$ d'où

$$x \equiv a_p (-1)^p + a_{p-1} (-1)^{p-1} + \dots + a_2 (-1)^2 + a_1 (-1) + a_0[11].$$

Conséquence :

- Si p est pair, alors

$$x \equiv a_p - a_{p-1} + a_{p-2} - \dots + a_2 - a_1 + a_0[11]$$

- Si p est impair, alors

$$x \equiv -a_p + a_{p-1} - \dots + a_2 - a_1 + a_0[11]$$

On a : $2357 \equiv 7[2] \Leftrightarrow 2357 \equiv 1[2]$; le reste est 1.

$2357 \equiv 7[5] \Leftrightarrow 2357 \equiv 2[5]$; le reste est 2.

$2357 \equiv 57[4] \Leftrightarrow 2357 \equiv 1[4]$; le reste est 1.

$2357 \equiv 2+3+5+7[3] \Leftrightarrow 2357 \equiv 17[3] \Leftrightarrow 2357 \equiv 2[3]$; le reste est 2.

$2357 \equiv 2+3+5+7[9] \Leftrightarrow 2357 \equiv 17[9] \Leftrightarrow 2357 \equiv 8[9]$; le reste est 8.

$2357 \equiv -2+3-5+7[11] \Leftrightarrow 2357 \equiv 3[11]$; le reste est 3.

2.5. Anneaux $(\mathbb{Z}/n\mathbb{Z}, +, \times)$:

Étudions la relation de congruence modulo 3.

Pour tout entier relatif a , on a soit $a \equiv 0[3]$ soit $a \equiv 1[3]$ soit $a \equiv 2[3]$.

$a \equiv 0[3]$	$a \equiv 1[3]$	$a \equiv 2[3]$
.	.	.
.	.	.
.	.	.
-9	-8	-7
-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
9	10	11
12	13	14
.	.	.
.	.	.
.	.	.

Soit $A = \{\dots; -6; -3; 0; 3; 6; \dots\}$, $B = \{\dots; -8; -5; -2; 1; 4; 7; \dots\}$ et $C = \{\dots; -4; -1; 2; 5; \dots\}$

On a :

- $A \neq \emptyset$, $B \neq \emptyset$ et $C \neq \emptyset$;
- $A \cap B = \emptyset$, $A \cap C = \emptyset$ et $B \cap C = \emptyset$;
- $A \cup B \cup C = \mathbb{Z}$.

Pour résumer ces trois points , on dit que A , B et C forment une partition de $\mathbb{Z}$.

La relation de congruence modulo 3 définit donc une partition de $\mathbb{Z}$ en trois parties appelées classes.

Pour dire que la classe d'un élément x de A est l'ensemble A dans la congruence modulo 3, on note $x \equiv A$ dans $\mathbb{Z}/3\mathbb{Z}$.

Exemples : Dans $\mathbb{Z}/3\mathbb{Z}$, on a :

$$\dot{6} = (-\dot{\hat{9}}) = \dot{0} = A$$

$$\dot{13} = (-\dot{\hat{5}}) = \dot{1} = B$$

$$\dot{20} = (-\dot{\hat{16}}) = \dot{2} = C$$

Plus généralement, soit n un nombre entier naturel non nul.

La partition de $\mathbb{Z}$ en n classes définie par la relation de congruence modulo n a donc pour éléments (les restes possibles de la division euclidienne par n) :

$$\dot{0} ; \dot{1} ; \dot{2} ; \dots ; \dot{\hat{n-2}} ; \dot{\hat{n-1}}.$$

L'ensemble de ces classes modulo n est noté $\mathbb{Z}/n\mathbb{Z}$.

Remarque :

Si $\dot{8} = \dot{2}$ dans $\mathbb{Z}/3\mathbb{Z}$, on a $\dot{8} = \dot{0}$ dans $\mathbb{Z}/2\mathbb{Z}$ et $\dot{8} = \dot{1}$ dans $\mathbb{Z}/7\mathbb{Z}$.

Propriétés :

$\forall n \in \mathbb{N} \setminus \{0; 1\}$ et $(x, y, z) \in (\mathbb{Z}/n\mathbb{Z})^3$, on a :

$$P1) \quad \dot{x} + \dot{y} = \dot{\hat{x+y}}$$

$$P2) \quad \dot{x} \times \dot{y} = \dot{\hat{x \times y}}$$

P3) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif et unitaire. (Voir notions préliminaires)

Remarque :

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau intègre si et seulement si n est un nombre premier.

Donc $\dot{x} \times \dot{y} = \dot{0} \Rightarrow \dot{x} = \dot{0}$ ou $\dot{y} = \dot{0}$ dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si n est **premier**.

Dressons les tables d'addition et de multiplication de $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$.

- Dans $\mathbb{Z}/6\mathbb{Z}$

+	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{5}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{0}$	$\dot{2}$	$\dot{4}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{2}$	$\dot{0}$	$\dot{4}$	$\dot{2}$
$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

On a : $\dot{2} \times \dot{3} = \dot{0}$ et $\dot{4} \times \dot{3} = \dot{0}$. Or $\dot{2} \neq \dot{3} \neq \dot{0}$.

Donc dans $\mathbb{Z}/6\mathbb{Z}$, $\dot{x} \times \dot{y} = \dot{0} \nRightarrow \dot{x} = \dot{0}$ ou $\dot{y} = \dot{0}$

- Dans $\mathbb{Z}/7\mathbb{Z}$

+	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{5}$	$\dot{5}$	$\dot{6}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{6}$	$\dot{6}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{1}$	$\dot{3}$	$\dot{5}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{6}$	$\dot{2}$	$\dot{5}$	$\dot{1}$	$\dot{4}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{1}$	$\dot{5}$	$\dot{2}$	$\dot{6}$	$\dot{3}$
$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{3}$	$\dot{1}$	$\dot{6}$	$\dot{4}$	$\dot{2}$
$\dot{6}$	$\dot{0}$	$\dot{6}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

Donc dans $\mathbb{Z}/7\mathbb{Z}$, $\dot{x} \times \dot{y} = \dot{0} \Rightarrow \dot{x} = \dot{0}$ ou $\dot{y} = \dot{0}$.

Activité :

Résoudre dans $\mathbb{Z}/6\mathbb{Z}$ puis dans $\mathbb{Z}/7\mathbb{Z}$ les équations suivantes :

- $\dot{2}x + \dot{3} = \dot{0}$
- $x^2 - \dot{5}x + \dot{6} = \dot{0}$

Première méthode : On fait un tableau avec les différentes classes.

- $\dot{2}x + \dot{3} = \dot{0}$

- Dans $\mathbb{Z}/6\mathbb{Z}$

x	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{2}x$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{0}$	$\dot{2}$	$\dot{4}$
$\dot{2}x + \dot{3}$	$\dot{3}$	$\dot{5}$	$\dot{1}$	$\dot{3}$	$\dot{5}$	$\dot{1}$

$$S = \emptyset$$

- Dans $\mathbb{Z}/7\mathbb{Z}$

x	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{2}x$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{1}$	$\dot{3}$	$\dot{5}$
$\dot{2}x + \dot{3}$	$\dot{3}$	$\dot{5}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{1}$

$$S = \{\dot{2}\}$$

- $x^2 - \dot{5}x + \dot{6} = \dot{0}$

- Dans $\mathbb{Z}/6\mathbb{Z}$

$$x^2 - \dot{5}x + \dot{6} = \dot{0} \Leftrightarrow x^2 - \dot{5}x = \dot{0}$$

x	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
x^2	$\dot{0}$	$\dot{1}$	$\dot{4}$	$\dot{3}$	$\dot{4}$	$\dot{1}$

$\dot{5}x$	$\dot{0}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$
$x^2 - \dot{5}x$	$\dot{0}$	$\dot{2}$	$\dot{0}$	$\dot{0}$	$\dot{2}$	$\dot{0}$

$$S = \{\dot{0}; \dot{2}; \dot{3}; \dot{5}\}$$

- Dans $\mathbb{Z}/7\mathbb{Z}$

x	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
x^2	$\dot{0}$	$\dot{1}$	$\dot{4}$	$\dot{2}$	$\dot{2}$	$\dot{4}$	$\dot{1}$
$\dot{5}x$	$\dot{0}$	$\dot{5}$	$\dot{3}$	$\dot{1}$	$\dot{6}$	$\dot{4}$	$\dot{2}$
$x^2 - \dot{5}x + \dot{6}$	$\dot{6}$	$\dot{2}$	$\dot{0}$	$\dot{0}$	$\dot{2}$	$\dot{6}$	$\dot{5}$

$$S = \{\dot{2}; \dot{3}\}$$

Deuxième méthode :

a) $\dot{2}x + \dot{3} = \dot{0}$

- Dans $\mathbb{Z}/6\mathbb{Z}$

$$\dot{2}x + \dot{3} = \dot{0} \Leftrightarrow \dot{2}x = -\dot{3} \Leftrightarrow \dot{2}x = \dot{3}$$

6 n'est pas un nombre premier. Alors on cherche les valeurs $x \in \{\dot{0}; \dot{1}; \dot{2}; \dot{3}; \dot{4}; \dot{5}; \dot{6}\}$ qui vérifient $\dot{2}x = \dot{3}$. Ce qui nous renvoie à la première méthode.

- Dans $\mathbb{Z}/7\mathbb{Z}$

$$\dot{2}x + \dot{3} = \dot{0} \Leftrightarrow \dot{2}x = -\dot{3} \Leftrightarrow \dot{2}x = \dot{4}$$

7 étant un nombre premier, il n'existe qu'une seule valeur $x \in \{\dot{0}; \dot{1}; \dot{2}; \dot{3}; \dot{4}; \dot{5}; \dot{6}\}$ qui vérifie $\dot{2}x = \dot{4}$ d'où $x = \dot{2}$.

$$S = \{\dot{2}\}$$

b) $x^2 - \dot{5}x + \dot{6} = \dot{0}$

- Dans $\mathbb{Z}/6\mathbb{Z}$

$$x^2 - \dot{5}x + \dot{6} = \dot{0} \Leftrightarrow x^2 - \dot{5}x = \dot{0}$$

$$\Leftrightarrow x(x - \dot{5}) = \dot{0}$$

6 n'étant pas premier, nous allons déterminer les valeurs de la table de multiplication de $\mathbb{Z}/6\mathbb{Z}$ dont le produit vaut $\dot{0}$.

$$\text{Dans } \mathbb{Z}/6\mathbb{Z}, \dot{0} \times \dot{a} = \dot{2} \times \dot{3} = \dot{4} \times \dot{3} = \dot{0}.$$

$$\text{Donc } x = \dot{0} \text{ ou } x - \dot{5} = \dot{0} \text{ ou } \begin{cases} x = \dot{2} \\ x - \dot{5} = \dot{3} \end{cases} \text{ ou } \begin{cases} x = \dot{3} \\ x - \dot{5} = \dot{2} \end{cases} \text{ ou } \begin{cases} x = \dot{4} \\ x - \dot{5} = \dot{3} \end{cases} \text{ ou } \begin{cases} x = \dot{3} \\ x - \dot{5} = \dot{4} \end{cases}$$

d'où

$$\diamond x = \dot{0}$$

$$\diamond x - \dot{5} = \dot{0} \Leftrightarrow x = \dot{5}$$

$$\diamond \begin{cases} x = \dot{2} \\ x - \dot{5} = \dot{3} \end{cases} \Leftrightarrow \begin{cases} x = \dot{2} \\ x - \dot{8} = \dot{2} \end{cases} \Leftrightarrow x = \dot{2}$$

$$\diamond \begin{cases} x = \dot{3} \\ x - \dot{5} = \dot{2} \end{cases} \Leftrightarrow \begin{cases} x = \dot{3} \\ x - \dot{7} = \dot{1} \end{cases} \text{ qui n'a pas de sens car } \dot{1} \neq \dot{3} \text{ dans } \mathbb{Z}/6\mathbb{Z}.$$

$$\diamond \begin{cases} x = \dot{4} \\ x - \dot{5} = \dot{3} \end{cases} \Leftrightarrow \begin{cases} x = \dot{4} \\ x - \dot{8} = \dot{2} \end{cases} \text{ qui n'a pas de sens car } \dot{2} \neq \dot{4} \text{ dans } \mathbb{Z}/6\mathbb{Z}.$$

$$\diamond \begin{cases} x = \dot{3} \\ x - \dot{5} = \dot{4} \end{cases} \Leftrightarrow \begin{cases} x = \dot{3} \\ x - \dot{9} = \dot{3} \end{cases} \Leftrightarrow x = \dot{3}$$

$$S = [\dot{0}; \dot{2}; \dot{3}; \dot{5}]$$

• Dans $\mathbb{Z}/7\mathbb{Z}$

$$x^2 - \dot{5}x + \dot{6} = \dot{0} \Leftrightarrow x^2 + \dot{2}x + \dot{6} = \dot{0}$$

$$\Leftrightarrow (x + \dot{1})^2 - \dot{1} + \dot{6} = \dot{0}$$

$$\Leftrightarrow (x + \dot{1})^2 + \dot{5} = \dot{0}$$

$$\Leftrightarrow (x + \dot{1})^2 - \dot{9} = \dot{0}$$

$$\Leftrightarrow (x + \dot{1})^2 - (\dot{3})^2 = \dot{0}$$

$$\Leftrightarrow (x + \dot{1} - \dot{3})(x + \dot{1} + \dot{3}) = \dot{0}$$

$$\Leftrightarrow (x - \dot{2})(x + \dot{4}) = \dot{0}$$

$$\Leftrightarrow x - \dot{2} = \dot{0} \text{ ou } x + \dot{4} = \dot{0} \text{ car } 7 \text{ est un nombre premier.}$$

$$\Leftrightarrow x = \dot{2} \text{ ou } x = -\dot{4} = \dot{3}$$

$$\text{d'où } S = [\dot{2}; \dot{3}].$$

Troisième méthode :

• Dans $\mathbb{Z}/7\mathbb{Z}$

$$x^2 - \dot{5}x + \dot{6} = \dot{0} \Leftrightarrow x^2 + \dot{2}x + \dot{6} = \dot{0}$$

$$\text{On a : } \Delta' = (\dot{1})^2 - \dot{6} = \dot{1} - \dot{6} = -\dot{5} = \dot{2} = (\dot{3})^2 = (\dot{4})^2$$

On prend $\dot{3}$ ou $\dot{4}$.

En prenant $\dot{3}$, on a :

$$x_1 = -\dot{1} - \dot{3} = -\dot{4} = \dot{3}$$

$$x_2 = -\dot{1} + \dot{3} = \dot{2}$$

En prenant $\dot{4}$, on a :

$$x_1 = -\dot{1} - \dot{4} = -\dot{5} = \dot{2}$$

$$x_2 = -\dot{1} + \dot{4} = \dot{3}$$

$$\text{d'où } S = [\dot{2}; \dot{3}]$$

3. PGCD et PPCM de deux entiers relatifs :

3.1. PPCM de deux entiers relatifs :

Soit a et b deux entiers relatifs non nuls.

On appelle plus petit multiple commun de a et b , noté $PPCM(a, b)$, le plus petit élément strictement positif des multiples communs à a et b .

Exemple : Déterminons $PPCM(5; 7)$.

On a :

$$5\mathbb{Z} = \{\dots; -5; 0; 5; 10; 15; 20; 25; 30; 35; 40; 45; 50; 55; 60; 65; 70; 75 \dots\}$$

$$7\mathbb{Z} = \{\dots; -7; 0; 7; 14; 21; 28; 35; 42; 49; 56; 63; 70; 77 \dots\}$$

$$PPCM(5; 7) = 35$$

Propriété :

Pour tous entiers relatifs a et b non nuls, on a :

$$PPCM(a, b) = PPCM(b, a) = PPCM(|a|, |b|)$$

$$\text{Donc } PPCM(5; 7) = PPCM(-7; 5) = PPCM(7; -5) = PPCM(-5; -7) = 35.$$

Propriété :

Pour tous entiers naturels a , b et k non nuls, on a :

$$P1) \quad \text{Max}(a, b) \leq PPCM(a, b) \leq ab$$

$$P2) \quad PPCM(a, b) = a \Leftrightarrow a \in b\mathbb{Z}$$

$$P3) \quad PPCM(ka, kb) = k \times PPCM(a, b)$$

$$\text{Donc } PPCM(15; 21) = 3 \times PPCM(5; 7) = 3 \times 35 = 105.$$

3.2. PGCD de deux entiers relatifs :

Activité :

On veut carreler une pièce rectangulaire de longueur 4,55 m et de largeur 3,85 m avec un nombre entier de dalles carrées sans aucune découpe.

a) Déterminer l'ensemble des diviseurs positifs de 455 et de 385.

- b) Déterminer l'ensemble des diviseurs positifs communs à 455 et 385.
 c) En déduire la mesure en *cm* du plus grand côté possible de dalles carrées pour carreler la pièce sans découpe.

Solution :

- a) Les diviseurs positifs de 455 et de 385.

$$\begin{array}{r|l} 455 & 5 \\ 91 & 7 \\ 13 & 13 \\ 1 & 1 \end{array} \quad \begin{array}{r|l} 385 & 5 \\ 77 & 7 \\ 11 & 11 \\ 1 & 1 \end{array}$$

On a : $455 = 5 \times 7 \times 13$.

Donc 455 admet $2 \times 2 \times 2 = 8$ diviseurs positifs qui sont :

$\{1; 5; 7; 13; 35; 65; 91; 455\}$.

De même $385 = 5 \times 7 \times 11$ admet 8 diviseurs positifs qui sont :

$\{1; 5; 7; 11; 35; 55; 77; 385\}$.

- b) Les diviseurs positifs communs à 455 et 385 sont :

$\{1; 5; 7; 35\}$.

- c) Le plus grand côté possible de dalles carrées.

La longueur de la pièce est $4,55 \text{ m} = 455 \text{ cm}$ et sa largeur $3,85 \text{ m} = 385 \text{ cm}$.

Le plus grand côté possible de dalles carrées est le plus grand diviseur commun à 455 et 385, c'est-à-dire 35 cm .

Synthèse :

Soit a et b deux entiers relatifs non tous nuls.

On appelle plus grand commun diviseur de a et b , noté $PGCD(a, b)$, le plus grand élément des diviseurs communs à a et b .

Exemple : Déterminons $PGCD(12; 32)$.

$$D(12) = \{-12; -6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 12\}$$

$$D(32) = \{-32; -16; -8; -4; -2; -1; 1; 2; 4; 8; 16; 32\}$$

Propriété :

Pour tous entiers relatifs non nuls a et b , on a :

$$PGCD(a, b) = PGCD(b, a) = PGCD(|a|, |b|)$$

$$\text{Donc } PGCD(12; 32) = PGCD(-12; 32) = PGCD(-32; 12) = PGCD(-12; -32) = 4.$$

Propriété :

Pour tous entiers naturels non nuls a , b et k , on a :

$$P1) \quad 1 \leq PGCD(a, b) \leq \min(a, b)$$

$$P2) \quad PGCD(a, b) = b \Leftrightarrow b \in D(a)$$

$$P3) \quad PGCD(ka, kb) = k \times PGCD(a, b)$$

$$\text{Donc } PGCD(24; 64) = 2 \times PGCD(12; 32) = 2 \times 4 = 8.$$

Propriété :

Soit a et b deux entiers naturels non nuls et δ leur $PGCD$.

Un entier relatif m est multiple de δ si et seulement si, il existe deux entiers relatifs u et v tels que : $m = au + bv$.

Propriété : Algorithme d'Euclide :

Soit a et b deux entiers naturels tels que $a > b > 0$ et r le reste de la division euclidienne de a par b .

- Si $r = 0$, alors $PGCD(a; b) = b$
- Si $r \neq 0$, alors $PGCD(a; b) = PGCD(b; r)$

Exemple : Déterminons $PGCD(2867; 3431)$

Dividend e	3431	2867	564
Diviseur	2867	564	47
Reste	564	47	0

$$PGCD(2867; 3431) = 47$$

3.3. Nombres premiers entre eux :

Soit a et b deux entiers relatifs non nuls.

On dit que a et b sont premiers entre eux si leur $PGCD$ est égal à 1.

Exemples :

3 et 5 sont premiers entre eux.

12 et 8 ne sont pas premiers entre eux.

Propriété :

Soit a , b et δ trois entiers relatifs non nuls tels que $\delta = PGCD(a; b)$.

Alors il existe deux entiers relatifs non nuls a' et b' tels que :

$$\begin{cases} a = \delta a' \\ b = \delta b' \\ \text{PGCD}(a'; b') = 1 \end{cases}$$

Théorème de Bézout :

Soit a et b deux entiers relatifs non nuls.

a et b sont premiers entre eux si et seulement si, il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Théorème de Gauss :

Soit a , b et c trois entiers relatifs non nuls.

Si a divise bc et si a et b sont premiers entre eux, alors a divise c .

Conséquences :

Soit a , b et c trois entiers relatifs non nuls.

- Si a et b sont premiers entre eux et si a et c sont premiers entre eux, alors a et bc sont premiers entre eux.
- Si a et b divisent c et si a et b sont premiers entre eux, alors ab divise c .
- Si a et b sont premiers entre eux, alors $\text{PPCM}(a; b) = ab$.

Propriété :

Soit n un entier naturel non nul et a , b , c trois entiers relatifs ($a \neq 0$).

Si a est premier avec n et si $ab \equiv ac [n]$, alors $b \equiv c [n]$.

Propriété :

Soit a et b deux entiers naturels non nuls, δ leur PGCD et m leur PPCM .

On a : $ab = \delta m$.

Activité :

Décomposer en produit de facteurs premiers 4312 et 6776 ; puis en déduire $\text{PGCD}(4312; 6776)$ et $\text{PPCM}(4312; 6776)$.

Solution :

$$\begin{array}{r|l}
 4312 & 2 \\
 2156 & 2 \\
 1078 & 2 \\
 539 & 7 \\
 77 & 7 \\
 11 & 11 \\
 1 &
 \end{array}
 \quad
 \begin{array}{r|l}
 6676 & 2 \\
 3388 & 2 \\
 1694 & 2 \\
 847 & 7 \\
 121 & 11 \\
 11 & 11 \\
 1 &
 \end{array}$$

On a : $4312 = 2^3 \times 7^2 \times 11$ et $6676 = 2^3 \times 7 \times 11^2$.

Donc $PGCD(4312; 6676) = 2^3 \times 7 \times 11 = 616$ et

$PPCM(4312; 6676) = 2^3 \times 7^2 \times 11^2 = 47432$.

Activité :

- En utilisant l'algorithme d'Euclide, déterminer deux entiers naturels x et y tels que : $45x - 28y = 1$.
- Résoudre dans $\mathbb{Z}^2$ l'équation (E) : $45x - 28y = 1$.
- Résoudre dans $\mathbb{Z}^2$ l'équation (E') : $45x - 28y = 6$.

Exercice :

- Résoudre dans $\mathbb{Z}$ le système : $\begin{cases} x \equiv 1[3] \\ x \equiv 2[7] \end{cases}$.
- Résoudre dans $\mathbb{N}^2$ les systèmes suivants :
 - $\begin{cases} PGCD(a; b) = 354 \\ a + b = 5664 \end{cases}$
 - $\begin{cases} PPCM(x; y) = 168 \\ x \times y = 1008 \end{cases}$
 - $\begin{cases} PPCM(x; y) = 504 \\ x + y = 135 \end{cases}$
 - $\begin{cases} PGCD(a; b) = 42 \\ PPCM(a; b) = 1680 \end{cases}$
- Soit a et b deux entiers naturels non nuls.
Démontrer que : $PGCD(13a + 8b; 5a + 3b) = PGCD(a; b)$.
- Soit n un entier relatif.
Démontrer que si 11 ne divise pas $(n-4)$, alors $(2n+3)$ et $(n+7)$ sont premiers entre eux.
- Déterminer les entiers relatifs n tels que la fraction $\frac{n+17}{n-1}$ soit un entier relatif.
- Divisibilité
 - Un nombre s'écrit $\overline{x43y}$ dans le système décimal. Déterminer x et y pour qu'il soit divisible par 2 et 9.
 - Un nombre s'écrit $\overline{28a75b}$ dans le système décimal. Déterminer a et b pour qu'il soit divisible par 3 et 11.

- c) Un nombre s'écrit $\overline{1c1dcd}$ dans le système décimal. Déterminer c et d pour qu'il soit divisible par 63.
7. On veut planter des arbres sur le périmètre d'un terrain triangulaire de côtés 132 m, 156 m et 204 m, de telle sorte qu'il y ait un arbre à chaque sommet du triangle et que les arbres soient également espacés.
Quel est le nombre minimum d'arbres que l'on pourra planter si l'on veut que la distance entre deux arbres soit exprimée en un nombre entier de mètres ?
8. Démontrer que pour tout entier naturel n , le nombre $n(2n+1)(7n+1)$ est divisible par 2 et par 3.
9. Soit n un entier naturel.
- Quels sont les restes possibles de la division euclidienne de n^4 par 5?
 - Démontrer que $n^5 - n$ est divisible par 5.
10. Résoudre dans $\mathbb{Z}$ les équations suivantes :
- $x^2 \equiv -1[5]$
 - $x^2 - 3x + 4 \equiv 0[7]$