Chapitre II
Divisibilité et Congruences

Table des matières

Partie A

Divisibilité dans $\mathbb{Z}$

1. Définitions

Définition 1. *Diviseur - Multiple*

Soit a et b deux entiers relatifs. On dit que b **divise** a et on note $b|a$ si :

$$\text{il existe } q \in \mathbb{Z} \text{ tel que } a = bq.$$

De manière équivalente, on dira également dans ce cas que :

- b est un **diviseur** de a, ou
- a est **divisible** par b, ou
- a est un **multiple** de b.

Exemple 1.

- -84 est un multiple de -28. En effet, $-84 = (-28) \times 3$.
- 2 divise tous les nombres pairs.
- 1 et -1 divisent tous les nombres entiers relatifs.
- 0 est multiple de tous les nombres entiers relatifs. Par contre, il ne divise que lui-même.

Exercice 1.

Donner tous les diviseurs de 24.

Correction.

$$-24, -12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12, 24.$$

Exercice 2.

1. Montrer que la somme de trois entiers relatifs consécutifs est divisible par 3.
   La somme de 2 entiers consécutifs est-elle divisible par 2 ?
2. (*) Soit $k \in \mathbb{N}^*$. Déterminer une condition nécessaire et suffisante pour que la somme de k entiers consécutifs soit divisible par k.

Correction.

1. Soit $n \in \mathbb{Z}$. Montrons que la somme S de n, de $n+1$ et de $n+2$ est divisible par 3.
   On a :
   $$S = n + (n+1) + (n+2) = n + n + n + 1 + 2 = 3n + 3 = 3(n+1).$$
   Ainsi, il existe $k \in \mathbb{Z}$ tel que $S = k \times 3$ (ici, $k = n+1$). Il en résulte que la somme de trois entiers consécutifs $S = n + (n+1) + (n+2)$ est divisible par 3.

   Par contre, la somme de 2 entiers consécutifs n'est pas divisible par 2. En effet, on a par exemple $1 + 2 = 3$ qui n'est pas divisible par 2.

2. Soit $n \in \mathbb{Z}$. Notons $S = n + (n+1) + \ldots + (n+k-1)$. Alors on a :
   $$S = kn + (1 + 2 + \ldots + k - 1) = kn + \frac{k(k-1)}{2} = k\left(n + \frac{k-1}{2}\right).$$
   On conjecture ainsi que notre condition nécessaire et suffisante est : *"k est un nombre impair"*.
   Montrons que notre conjecture est bonne.
   — Montrons que la condition est suffisante. Supposons que k est impair. Alors il existe $p \in \mathbb{N}$ tel que $k = 2p + 1$. Par suite, d'après ce qui précède :
   $$S = k\left(n + \frac{k-1}{2}\right) = k\underbrace{(n+p)}_{\in\mathbb{Z}}$$
   donc $k|S$.
   — Montrons que la condition est nécessaire. On suppose $k|S$. Alors il existe $m \in \mathbb{Z}$ tel que $S = km$. D'après la remarque initiale, on a donc $k\left(n + \frac{k-1}{2}\right) = S = km$. Or $k \neq 0$, donc $n + \frac{k-1}{2} = m$. Ainsi, on a :
   $$k = 2\underbrace{(m-n)}_{\in\mathbb{Z}} + 1$$
   d'où k est un nombre impair.
   On a donc prouvé que la somme de k entiers consécutifs est divisible par k si, et seulement si, k est un nombre impair.

Notation 1.

Soit n un entier relatif. On note
$$n\mathbb{Z} = \{\ldots - 3n, -2n, -n, 0, n, 2n, 3n, \ldots\} = \{nk \mid k \in \mathbb{Z}\},$$
l'ensemble des multiples de n.
Par exemple, $4\mathbb{Z} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$

Exercice 3.

1. Comment appelle-t-on d'habitude l'ensemble $2\mathbb{Z}$?
2. Déterminer l'ensemble $-2\mathbb{Z}$, l'ensemble $1\mathbb{Z}$ puis l'ensemble $0\mathbb{Z}$.

3. Montrer que $12\mathbb{Z} \subset 4\mathbb{Z}$.
4. $(*)$ Soit $n, m \in \mathbb{Z}$. Montrer que m divise n si, et seulement si, $n\mathbb{Z} \subset m\mathbb{Z}$.

Correction.

1. $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\} = \{..., -8, -6, -4, -2, 0, 2, 4, 6, 8, ...\}$ est connu sont le nom d'ensemble des nombres pairs.
2. — $-2\mathbb{Z} = 2\mathbb{Z}$;
   — $1\mathbb{Z} = \mathbb{Z}$;
   — $0\mathbb{Z} = \{0\}$.
3. Soit $p \in 12\mathbb{Z}$. Alors, p est un multiple de 12 i.e. il existe $k \in \mathbb{Z}$ tel que $p = 12k$.
   Or on a :
   $$p = 12k = (4 \times 3)k = 4 \times \underbrace{3k}_{\in\mathbb{Z}};$$
   donc p est un multiple de 4 - i.e. il existe $k' \in \mathbb{Z}$ tel que $p = 4k'$ (ici $k' = 3k$).
   Il en résulte que p appartient à $4Z$.
   Ceci étant vrai quelque soit $p \in 12\mathbb{Z}$, on en déduit que $12\mathbb{Z} \subset 4\mathbb{Z}$.
4. Soit $n, m \in \mathbb{Z}$. Ici, on cherche à montrer une équivalence ("si, et seulement, si" $= \Leftrightarrow$) : on doit donc montrer deux implications :
   — $(\Rightarrow)$: Si m divise n, alors $n\mathbb{Z} \subset m\mathbb{Z}$.
   On suppose que m divise n. Montrons que $n\mathbb{Z} \subset m\mathbb{Z}$.
   Soit $p \in n\mathbb{Z}$. Alors il existe $k \in \mathbb{Z}$ tel que $p = nk$. Or, par hypothèse, m divise n. Alors il existe $k' \in \mathbb{Z}$ tel que $n = mk'$. Par suite, on a :
   $$p = nk = (mk')k = m\underbrace{(k'k)}_{\in\mathbb{Z}}.$$
   Par suite, il existe $k'' \in \mathbb{Z}$ tel que $p = mk''$. Donc $p \in m\mathbb{Z}$.
   Il en résulte que $n\mathbb{Z} \subset m\mathbb{Z}$.
   — $(\Leftarrow)$: Si $n\mathbb{Z} \subset m\mathbb{Z}$, alors m divise n.
   On suppose que $n\mathbb{Z} \subset m\mathbb{Z}$. Montrons que m divise n.
   Comme $n \in n\mathbb{Z}$ et $n\mathbb{Z} \subset m\mathbb{Z}$, alors $n \in m\mathbb{Z}$. Par suite, il existe $k \in \mathbb{Z}$ tel que $n = mk$.
   Il en résulte que m divise n.
   On a montré les deux implications de l'équivalence, et ainsi, on a montré que m divise n si, et seulement si, $n\mathbb{Z} \subset m\mathbb{Z}$.

2. Propriétés

Proposition 1.

Soit a, b des entiers relatifs.

- Si b divise a et $a \neq 0$, alors $|b| \leq |a|$.
- Si b divise a et a divise b, alors $a = b$ ou $a = -b$.

Démonstration.

Soit $a, b \in \mathbb{Z}$.

- On suppose que b divise a et $a \neq 0$. Montrons que $|b| \leq |a|$.
  Comme b divise a, il existe $k \in \mathbb{Z}$ tel que $a = bk$. Or $a \neq 0$, donc $k \neq 0$. Ainsi, $|k| \geq 1$ d'où :
  $$|a| = |bk| = |b|. \underbrace{|k|}_{\geq 1} \geq |b|.$$

bu On suppose que b divise a et a divise b. Montrons que $a = \pm b$.
D'après la propriété précédente, comme b divise a, alors $|b| \leq |a|$. De même, comme a divise b, alors $|a| \leq |b|$. Par suite,
$$|a| = |b|.$$
Il en résulte que $a = b$ ou $a = -b$.

□

Théorème 1. *Transitivité*

Soit a, b, c des entiers relatifs. Si c divise b et b divise a, alors c divise a.

Démonstration.

Soit $a, b, c \in \mathbb{Z}$. On suppose que c divise b et b divise a. Montrons que c divise a.
Comme c divise b, alors il existe $k \in \mathbb{Z}$ tel que $b = kc$ et comme b divise a, alors il existe $k' \in \mathbb{Z}$ tel que $a = k'b$. Par suite, on a :

$$a = k'b = k'(kc) = \underbrace{k'k}_{\in \mathbb{Z}} c.$$

Il en résulte que c divise a. □

Théorème 2. *Combinaison linéaire*

Soit a, b et d des entiers relatifs. Si d divise a et d divise b, alors, pour tous $u, v \in \mathbb{Z}$, d divise $ua + vb$.

Correction.

Soit $a, b, d \in \mathbb{Z}$. On suppose que d divise a et d divise b. Montrons que, pour tous $u, v \in \mathbb{Z}$, d divise $ua + vb$.
Soit $u, v \in \mathbb{Z}$. Comme d divise a, alors il existe $k \in \mathbb{Z}$ tel que $a = kd$ et comme d divise b, alors il existe $k' \in \mathbb{Z}$ tel que $b = k'd$. Par suite, on a :

$$ua + vb = u(kd) + v(k'd) = \underbrace{(uk + vk')}_{\in \mathbb{Z}} d.$$

Il en résulte que d divise $ua + vb$.

Exemple 2.

Si d est un diviseur commun de a et b alors d divise $a \pm b$.

3. Représentations des nombres entiers naturels en base 10

a. Écriture d'un nombre en base 10

Lemme 1.

Soit N un entier naturel. Il existe une unique suite $(a_k)_{k\in\mathbb{N}}$ stationnaire en 0 et à valeurs dans $\{0,1,2,3,4,5,6,7,8,9\}$ telle que :

$$N = a_0 + a_1 \times 10 + \ldots + a_k \times 10^k + \ldots \quad \text{(somme finie)}$$

Exemple 3.

- Le nombre ||||||||||| se décompose :

$$||||||||||| = \underbrace{2}_{a_0} + \underbrace{1}_{a_1} \times 10 + \underbrace{0}_{a_2} \times 10^2 + \underbrace{0}_{a_3} \times 10^3 + \ldots$$

- Le nombre |||| se décompose :

$$|||| = \underbrace{4}_{a_0} + \underbrace{0}_{a_1} \times 10 + \underbrace{0}_{a_2} \times 10^2 + \underbrace{0}_{a_3} \times 10^3 + \ldots$$

- Le nombre 1325 se décompose :

$$1325 = \underbrace{5}_{a_0} + \underbrace{2}_{a_1} \times 10 + \underbrace{3}_{a_2} \times 10^2 + \underbrace{1}_{a_3} \times 10^3 + \underbrace{0}_{a_4} \times 10^4 + \underbrace{0}_{a_5} \times 10^5 + \ldots$$

Définition 2.

Soit N un entier naturel non nul. On appelle représentation en base 10 (ou décimale) du nombre N la notation :

$$N = a_n a_{n-1} \ldots a_1 a_0 \text{ ou encore } \overline{a_n a_{n-1} \ldots a_1 a_0}^{10}$$

où $N = a_0 + a_1 \times 10 + \ldots + a_n \times 10^n$ avec $a_n \neq 0$ et les a_k dans $[\![0,9]\!]$.

On définit la représentation en base 10 (ou décimal) du nombre nul par 0 ou encore $\overline{0}^{10}$.

Exemple 4.

Représentons en base 10 les nombres de l'exemple précédent :

- Le nombre ||||||||||| s'écrit, en base 10 :

$$||||||||||| = 12$$

- Le nombre |||| s'écrit, en base 10 :
$$|||| = 4$$
- Le nombre 1325 s'écrit, en base 10, suspens :
$$1325 = 1325$$

Exercice 4.

Soit a, b, c, d des entiers compris entre 0 et 9. On considère les entiers A et B dont les écritures décimales sont respectivement :

$$A = \overline{abcd}^{10} \quad \text{et } B = \overline{bcad}^{10}$$

Montrer que $A - B$ est divisible par 9.

Correction.

On a :

$$\begin{array}{rcl} A - B & = & a \times 10^3 + b \times 10^2 + c \times 10 + d - (b \times 10^3 + c \times 10^2 + a \times 10 + d) \\ & = & 990a - 900b - 90c \\ A - B & = & 9 \times \underbrace{(110a - 100b - 10c)}_{\in \mathbb{Z}} \end{array}$$

donc 9 divise $A - B$.

Exercice 5.

Exercices 14,15 p126.

b. Quelques règles de divisibilité

Exercice 6.

Donner, sans démonstration, les règles générales qui permettent de savoir si un nombre entier relatif écrit en base 10 est divisible par :

1. le nombre 2 ;
2. le nombre 5 ;
3. les nombres 10, 100, ... , 10^n où $n \in \mathbb{N}$;
4. le nombre 3 ;
5. le nombre 9 ;
6. pour des entiers de 2 ou 3 chiffres, le nombre 11.

Correction.

1. Tout nombre entier relatif finissant par $0, 2, 4, 6$ ou 8 est divisible par 2.
2. Tout nombre entier relatif finissant par 0 ou 5 est divisible par 5.
3. Tout nombre entier relatif finissant par n zéros est divisible par 10^n.
4. Tout nombre entier relatif dont les sommes successives des chiffres aboutissent à $3, 6$ ou 9 est divisible par 3.
5. Tout nombre entier relatif dont les sommes successives des chiffres aboutissent à 9 est divisible par 9.
6. Tout nombre entier relatif de deux chiffres égaux est divisible par 11 et tout nombre entier relatif de trois chiffres dont la somme des deux chiffres extrêmes est égal au chiffre central est divisible par 11.

4. Exercices

Voici quelques exercices classiques de divisibilité :

Exercice 7. *Couple d'entiers satisfaisant une équation*

On considère l'équation d'inconnues x et y :

$$x^2 = 15 + 2xy.$$

Existe-t-il des couples (x, y) d'entiers naturels qui sont solutions de l'équation précédente ?

Le principe est de résolution de ce genre d'exercices est le suivant :

- On transforme l'équation de telle sorte qu'on puisse trouver :
  - dans le membre de gauche, tous les termes faisant apparaître x et y ;
  - dans le membre de droite, tous les termes constants - dans ces exercices, il s'agira obligatoirement d'un **nombre entier**.
- On factorise le membre de gauche (celui avec les x et y de telle sorte qu'on puisse faire apparaître 2 facteurs (ou plus).
  les inconnues x et y étant supposées entières, les facteurs précédents le sont aussi. Ce sont donc des diviseurs de l'entier présent dans le membre de droite.
- On établit la liste des diviseurs du membre de droite et on réunit ceux dont le produit est égal au membre de droite.
- Finalement, on fait correspondre les facteurs du membre de gauche avec chaque réunion de diviseurs et on résout les systèmes obtenus.

Correction.

L'équation $x^2 = 15 + 2xy$ est équivalente à :

$$x^2 - 2xy = 15 \quad \Leftrightarrow \quad x(x - 2y) = 15$$

Les diviseurs dans $\mathbb{N}$ de 15 sont $1, 3, 5$ et 15. Les décompositions de 15 en produits de deux

facteurs entiers sont donc :

$$15 \times 1 \text{ ou } 1 \times 15 \text{ ou } 5 \times 3 \text{ ou } 3 \times 5.$$

On remarque de plus, que comme x, y sont positifs, $x \geq x - 2y$ donc les seuls décompositions possibles de la forme $x(x-2y)$ sont :

$$\begin{cases} x & = 15 \\ x - 2y & = 1 \end{cases} \text{ ou } \begin{cases} x & = 5 \\ x - 2y & = 3 \end{cases}$$

On en déduit :

$$\begin{cases} x & = 15 \\ y & = 7 \end{cases} \text{ ou } \begin{cases} x & = 5 \\ y & = 1 \end{cases}$$

Ainsi, les seuls couples (x, y) d'entiers naturels solutions de $x^2 = 15 + 2xy$ sont $(15, 7)$ et $(15, 1)$.

Exercice : Exercices 12p 126 ; 60 p127

Exercice 8.

Déterminer tous les nombres entiers relatifs n tels que $3n + 2$ divise $4n + 1$.

Le principe est de résolution de ce genre d'exercices est le suivant :

- On cherche une combinaison linéaire des deux termes de l'énoncé qui élimine la variable n recherchée ;
- On utilise le théorème 2 sur les combinaisons linéaires pour obtenir un relation de divisibilité avec un nombre entier relatif simple.
- On établit la liste des diviseurs de cet entier, et on vérifie, pour chaque diviseur, s'il fait l'affaire.

Correction.

On suppose que $3n + 2$ divise $4n + 1$. Comme, de plus, $3n + 2$ divise $3n + 2$, d'après le théorème 2, $3n + 2$ divise la combinaison linéaire :

$$4(3n + 2) - 3(4n + 1) = 12n - 12n + 8 - 3 = 5.$$

Ainsi, $3n + 2$ divise 5. Or 5 admet quatre diviseurs dans $\mathbb{Z}$:

$$-5, -1, 1, 5.$$

Par suite, on a les possibilités suivantes :

— $3n + 2 = -5$ ce qui implique $n = \frac{-7}{3}$. Impossible !

— $3n+2=-1$ ce qui implique $n=-1$.
— $3n+2=1$ ce qui implique $n=\frac{-1}{3}$. Impossible !
— $3n+2=5$ ce qui implique $n=1$.

Ainsi, les deux solutions potentielles sont $n=-1$ et 1. On vérifie alors que ces valeurs conviennent bien :

— $3\times(-1)+2=-1$ divise $-3=4\times(-1)+1$ donc $n=-1$ est bien solution ;
— $3\times 1+2=5$ divise $5=4\times 1+1$ donc $n=1$ est bien solution.

Exercice corrigé : Exercice 4 p117
Exercices : Exercice 10 p126 ; 59 p129

Partie B

Division euclidienne

1. La division euclidienne

La division euclidienne est l'un des outils principaux de l'arithmétique.

a. La division euclidienne dans $\mathbb{N}$

Théorème 3. *Division euclidienne dans $\mathbb{N}$*

Soit a, b des entiers **naturels** tels que $b \neq 0$.
Il existe un **unique** couple (q, r) d'entiers naturels tels que :

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

Démonstration.

Soit $a, b \in \mathbb{N}$ tels que $b \neq 0$.

- **Existence.** On considère le sous-ensemble M de $\mathbb{N}$ suivant :

  $$M = \{k \in \mathbb{N} \mid bk \leq a\}.$$

  Comme $b \neq 0$, M est majoré par le premier entier supérieur au nombre rationnel $\frac{a}{b}$ (il s'agit de l'entier $E\left(\frac{b}{a}\right) + 1$). Et de plus, M est non vide car $0 \in M$.
  Ainsi, M est une partie non vide et majorée de $\mathbb{N}$; elle admet donc un plus grand élément q. *On admet ici le résultat : toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.*
  Par suite, bq est le plus grand multiple de b inférieur ou égal à a et donc on a :

  $$bq \leq a < b(q+1).$$

  En posant $r = a - bq$, on obtient, en retranchant bq dans l'inégalité précédente :

  $$0 \leq r < b.$$

  et on a bien $bq + r = bq + (a - bq) = a$.

- **Unicité.** Supposons que les couples (q, r) et (q', r') vérifient :

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

  Alors :

  $$0 = a - a = b(q - q') + (r - r'),$$

  d'où $b(q' - q) = r - r'$.
  Par suite, $r - r'$ est un multiple de b qui vérifie $-b < r - r' < b$. Or 0 est le seul multiple

de b strictement compris entre $-b$ et b.
Donc $0 = r - r' = b(q' - q)$. Ainsi $r = r'$ et $q = q'$ (car $b \neq 0$).
Il en résulte qu'il n'existe qu'un seul couple (q, r) d'entiers naturels tels que :

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

□

Remarque 1.

Dans la division euclidienne de a par b - $a = bq + r$ avec $0 \leq r < b$:

- a est appelé le **dividende** ;
- b est appelé le **diviseur** ;
- q est appelé le **quotient** ;
- r est appelé le **reste** ;

Exercice 9.

En utilisant les souvenirs enfouis dans votre mémoire, effectuer, à la main, les divisions euclidiennes suivantes :

12 par 5; 129 par 11; 4237 par 7;

b. Algorithme de la division euclidienne dans $\mathbb{N}$

Algorithme de la division euclidienne dans $\mathbb{N}$

```
def division_euclidienne(a,b):
    r=a
    q=0
    while r<b:
        r=r-b
        q=q+1
    return q,r
```

c. La division euclidienne dans $\mathbb{Z}$

On admettra le théorème suivant :

Théorème 4. *Division euclidienne dans $\mathbb{Z}$*

Soit a, b des entiers **relatifs** tels que $b \neq 0$.
Il existe un **unique** couple (q, r) d'entiers naturels tels que :

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

Exercice 10.

Déterminer les restes et quotients de la division euclidienne de :

$$-15 \text{ par } 4 \qquad -36 \text{ par } -10$$

Correction.

On a $-15 = 4 \times (-4) + 1$ avec $0 \leq 1 \leq 4$;
On a $-36 = (-10) \times 4 + 4$ avec $0 \leq 4 \leq |-10| = 10$;

Exercice 11.

Exercices 23 p126, 25,28p 127

2. Techniques de démonstration

a. Techniques de démonstration : la disjonction de cas

La disjonction de cas : il arrive parfois que ce que l'on souhaite démontrer dépende d'un paramètre disons c et que la preuve varie selon la valeur de ce paramètre. On sépare alors le raisonnement en plusieurs cas que l'on démontre séparément et on parlera de raisonnement par **disjonction de cas**. On fera bien attention à l'exhaustivité des cas !

Exercice 12. *Exercice sur la disjonction de cas*

Montrer que pour tout $n \in \mathbb{N}$, $n(n+1)(n+2)$ est divisible par 3.

Correction.

Soit $n \in \mathbb{Z}$. On effectue la division euclidienne de n par 3. Alors il existe un unique couple d'entiers (q, r) tels que $n = 3q + r$ avec $0 \leq r < 3$.
Le reste r prennant 3 valeurs : 0,1, ou 2, on a alors 3 cas possibles. On effectue ainsi, une **disjonction de cas** :

- *1er cas :* $r = 0$
  Alors $n = 3k$ et on a :
  $$n(n+1)(n+2) = 3\underbrace{q(3q+1)(3q+2)}_{\in\mathbb{Z}}$$
  Donc dans ce cas 3 divise $n(n+1)(n+2)$
- *2eme cas :* $r = 1$
  Alors $n = 3k$ et on a :
  $$n(n+1)(n+2) = (3q+1)(3q+2)(3q+3) = 3\underbrace{(3q+1)(3q+2)(q+1)}_{\in\mathbb{Z}}$$

Donc dans ce cas 3 divise $n(n+1)(n+2)$

— *3eme cas :* $r = 2$
Alors $n = 3k$ et on a :

$$n(n+1)(n+2) = (3q+2)(3q+3)(3q+4) = 3\underbrace{(3q+2)(q+1)(3q+4)}_{\in\mathbb{Z}}$$

Donc dans ce cas 3 divise $n(n+1)(n+2)$

Dans tous les cas 3 divise $n(n+1)(n+2)$.
Il en résulte que pour tout $n \in \mathbb{N}$, 3 divise $n(n+1)(n+2)$.

Exercice Exercice 29 p127, 61 p129

b. Techniques de démonstration : la contraposition

La contraposée : la contraposée d'une implication $P \Rightarrow Q$ est l'implication non $Q \Rightarrow$ non P. Ces deux implications ont la même valeur de vérité : ainsi, pour démontrer que l'implication $P \Rightarrow Q$ est vraie l'implication on peut démontrer l'implication non $Q \Rightarrow$ non P si elle nous semble plus faisable. On dit alors que l'on effectue un raisonnement par **contraposition**.

En voici un exemple typique en arithmétique :

Exercice 13. *Exercice sur la contraposition*

1. Soit $n \in \mathbb{Z}$.
   (a) Montrer que si n^2 est pair alors n est pair.
   (b) Montrer que si n^2 est impair alors n est impair.
2. En déduire que si a, b sont des entiers naturels tels que $a^2 - 2b^2 = 1$, alors a est impair et que b est pair.

Correction.

1. (a) Montrons que si n^2 est pair alors n est pair. Raisonnons par contraposition en montrant l'implication contraposée : si n est impair alors n^2 est impair.
   On suppose n impair. Alors il existe $k \in \mathbb{Z}$ tel que $n = 2k+1$ et ainsi :

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2\underbrace{(2k^2+2k)}_{\in\mathbb{Z}} + 1$$

   Par suite n^2 est impair.
   Ainsi, par contraposée, on a montré que si n^2 est pair alors n est pair.

   (b) Montrons que si n^2 est impair alors n est impair. Raisonnons par contraposition en montrant l'implication contraposée : si n est pair alors n^2 est pair.

On suppose n impair. Alors il existe $k \in \mathbb{Z}$ tel que $n = 2k$ et ainsi :

$$n^2 = (2k)^2 = 4k^2 = 2\underbrace{(2k^2)}_{\in\mathbb{Z}}$$

Par suite n^2 est pair.
Ainsi, par contraposée, on a montré que si n^2 est impair alors n est impair.

2. Soit a, b des entiers naturels tels que $a^2 - 2b^2 = 1$. Alors on a :

$$a^2 = 2b^2 + 1$$

donc a^2 est impair. Par suite, d'après le raisonnement par contraposée 1. b) qui précède, a est impair.
Ainsi, il existe $k \in \mathbb{Z}$ tel que $a = 2k + 1$. Par suite, on a :

$$2b^2 = a^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 2\underbrace{(2k^2 + 2k)}_{\in\mathbb{Z}}$$

donc b^2 est pair. Par suite, d'après le raisonnement par contraposée 1. a) qui précède, b est impair.

Exercice 14.

Soit $x, y \in \mathbb{R}$.

1. Montrer que si $x + y$ est irrationnel, alors x est irrationnel ou y est irrationnel.
2. Montrer que si xy est irrationnel, alors x est irrationnel ou y est irrationnel.

Correction.

3. Exercices

Exercice 15.

Soit n un entier naturel. Pour quelle(s) valeur(s) de n, le reste de la division euclidienne de $(n+2)^3$ par n^2 est $12n + 8$?

Correction.

Soit $n \in \mathbb{N}$. On a :

$$(n+2)^3 = n^3 + 6n^2 + 12n + 8 = n^2(n+6) + 12n + 8$$

Donc $12n + 8$ est le reste de la division euclidienne de $(n+2)^3$ par n^2 est $12n + 8$ lorsqu'on a la relation que doit vérifier le reste, c'est-à-dire : $0 \leq 12n + 8 < n^2$.
Comme $n \in \mathbb{N}$, $12n + 8 \geq 0$ et on remarque que $12n + 8 < n^2$ si, et seulement si, $n^2 - 12n - 8 > 0$,

ce qui nous donne l'idée d'étudier le signe de la fonction $f : x \mapsto x^2 - 12n - 8$ sur $\mathbb{R}$. Il s'agit d'une fonction polynomiale du second degré et en utilisant la méthode du discriminant, on détermine les deux racines $x_1 \simeq -0.6$ et $x_2 \simeq 12,6$ de f. On obtient alors que :

$$f(x) > 0 \text{ si, et seulement si, } x \in]-\infty, x_1[\cup]x_2, +\infty[.$$

Or n est un **entier positif** donc $f(n) > 0$ si, et seulement si, $n \geq 13$. Ainsi, dès que $n \geq 13$, $12n + 8$ est le reste de la division euclidienne de $(n+2)^3$ par n^2.

Exercice 16.

Exercice 69 p129

Exercice 17. *(*)*

Soit n un entier naturel. Montrer que si $n^2 - 1$ n'est pas un multiple de 8, alors n est pair.

Exercice 18. *(*)*

Soit n un entier naturel et r le reste de la division euclidienne de n par 4. Montrer que si n est la somme de deux carrés, alors $r \neq 3$.

Partie C

Congruences

1. Activité d'introduction

Question.

Quel était jour de la semaine lors du 14 Juillet 1789 ?

Le 14 Juillet 2023 était un vendredi. Comment en déduire le jour de la semaine du 14 Juillet 1789 ?

- Combien d'années se sont écoulées entre le 14/07/1789 et le 14/07/2023 ?
- Combien de jours se sont écoulés entre ces deux dates ? **Attention !** Il faut tenir compte des années bissextiles ! Les années bissextiles sont :
  — l'ensemble des années qui sont multiples de 4 ;
  — auquel on enlève l'ensemble des années qui sont multiples de 100 ;
  — auquel on rajoute l'ensemble des années qui sont multiples de 400.
- Comment déduire de ce nombre de jours écoulés le jour de la semaine recherché ? Puis comment conclure sur le jour de la semaine recherché ?
- Déduire de cet exemple un moyen de déterminer le jour de la semaine de n'importe quelle date !

  Attention ! Pour employer la définition des années bissextiles utilisée plus haut, l'année de la date choisie doit être supérieure à 1582.

Correction.

- $2020 - 1789 = 231$ années se sont écoulées.
- Une année "normale" comportant 365 jours, on a donc 231×365 jours écoulés entre les deux dates **sans compter les jours apportés par les années bissextiles**. Chaque année bissextile ajoutant 1 jour par rapport à une année normale, il suffit donc de compter les nombre d'années bissextiles pour connaître le nombre de jours que l'on doit ajouter à notre premier décompte (231×365) pour qu'il soit correct. Comptons ce nombre d'années bissextiles : nous devons, trois fois de suite, compter le nombre de multiples de $n = 4, 100, 400$ compris entre les années correspondant aux deux dates.
  Attention, il faut bien penser à vérifier les années de chaque date doivent être comprises dans notre décompte des multiples ou non selon que le 29 février est passé ou non pour chacune de ces dates ; ici, le souci ne se pose pas car ces années ne sont pas des multiples de n et nous verrons comment gérer ces cas sur des exemples concrets.
  Il faut, pour calculer le nombre de multiples de n entre 1789 et 2020 :
  — calculer le nombre de multiple de n compris entre 1 et 2020 ce qui correspond donc quotient de la division euclienne de 2020 par n. Ce quotient est obtenu par le calcul

suivant : $E\left(\frac{2020}{n}\right)$ où E désigne la fonction partie entière ;

— puis retrancher le nombre de multiple de n compris entre 1 et 1789 soit $E\left(\frac{1789}{n}\right)$

Ainsi, on obtient les nombres suivants :

— Nombre de mutiples de 4 : $E\left(\frac{2020}{4}\right) - E\left(\frac{1789}{4}\right) = 58.$

— Nombre de mutiples de 100 : $E\left(\frac{2020}{100}\right) - E\left(\frac{1789}{100}\right) = 3.$

— Nombre de mutiples de 400 : $E\left(\frac{2020}{400}\right) - E\left(\frac{1789}{400}\right) = 1.$

Et donc, le nombre d'années bissextiles (et donc de jours à ajouter dans notre décompte initial) est égal à $58 - 3 + 1 = 56$.

Le nombre de jours J entre les deux dates est donc égal à

$$J = 231 \times 365 + 56 = 84371.$$

on verra que lorsque l'on maîtrisera les congruences et leurs propriétés, on pourra s'arrêter à l'expression $231 \times 365 + 56$ pour le nombre de jours afin d'obtenir plus efficacement le reste voulu !

Maintenant, pour savoir quel était le jour de la semaine de notre date de départ, on remarque que le nombre de semaines écoulées n'est pas important et que seuls les jours restants une fois toutes les semaines écoulées enlevée ont une "influence" sur le résultat !
Une semaine comportant 7 jours, on calcule donc le reste r de la division euclidienne de $J = 84371$ par 7 : on obtient $r = 0$.
Ainsi, le jour de la semaine du 14 Juillet 1789 tombe le même jour que le 14 juillet 2020 qui était un mardi. **La Prise de la Bastille a donc eu lieu un Mardi !**

Exercice 19.

Déterminer le jour de la semaine de votre date de naissance !

Voire les exercices 80,81 p131.

2. Définitions et exemples

Définition 3. *Congruence modulo un entier naturel*

Soit m un entier naturel non nul et a, b deux entiers relatifs.
On dit que a **est congru à** b **modulo** m et on écrit :

$$a \equiv b \mod m \qquad \text{ou} \qquad a \equiv b \ [m]$$

si a et b ont le **même reste** dans leur division euclidienne par m.

Exemple 5.

- $25 \equiv 1 \mod 6$ et $251 \equiv 37 \mod 2$
- Deux dates du calendrier ont lieu le même jour de la semaine si, et seulement si, le nombre J de jours écoulés entre ces deux dates vérifie :

$$J \equiv 0 \mod 7$$

Exercice 20.

Remplir avec les congruences suivantes avec le plus petit nombre entier naturel possible :

$$81 \equiv \ldots \mod 9 \qquad 58 \equiv \ldots \mod 15 \qquad 1221 \equiv \ldots \mod 4 \qquad 10^{200} \equiv \ldots \mod 1.$$

Correction.

On a :

$$81 \equiv 0 \mod 9 \qquad 58 \equiv 13 \mod 15 \qquad 1221 \equiv 1 \mod 4 \qquad 10^{200} \equiv 0 \mod 1.$$

3. Propriétés

Proposition 2.

Soit m un entier naturel non nul et a, b deux entiers relatifs. On a $a \equiv b \mod m$ si, et seulement si, $b - a$ est un multiple de m.

Démonstration.

On considère les quotients et restes de la division euclidienne de a par m et de b par m : il existe un unique couple (q, r) et un unique couple (q', r') d'entiers relatifs avec $0 \leq r < a$ et $0 \leq r' < b$ tels que :

$$a = mq + r \quad \text{et } b = mq' + r'.$$

- On suppose que $a \equiv b \mod m$. Montrons que $a - b$ est un multiple de n.
  Comme $a \equiv b \mod m$, on a $r = r'$. Ainsi,

$$a - b = mq + r - (mq' + r') = m(q - q') + r - r' = m\underbrace{(q - q')}_{\in \mathbb{Z}}$$

  Par suite, $a - b$ est un multiple de m.
- On suppose que $a - b$ est un multiple de m. Montrons que $a \equiv b \mod m$.
  Comme $a - b$ est un multiple de m, il existe $k \in \mathbb{Z}$ tel que $a - b = mk$. Par suite, on a $mk = a - b = m(q - q') + r - r'$ et donc :

$$r - r' = m(k - q + q')$$

  Par suite, m divise $r - r'$. Or on a $-m < r - r' < m$ donc $r - r' = 0$. D'où $r = r'$. Il en résulte que $a \equiv b \mod m$.

□

Exercice 21.

Soit $m \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Montrer que $a \equiv 0 \bmod m$ si, et seulement si, a est un multiple de m.

Correction.

En utilisant la proposition précédente, on peut conclure immédiatement car $a \equiv 0 \bmod m$ si, et seulement si, $a = a - 0$ est un multiple de m.

Montrons tout de même directement cette équivalence : On considère la division euclidienne de a par m : il existe un unique couple d'entiers relatifs (q, r) avec $0 \leq r < m$ tel que :

$$a = mq + r.$$

- On suppose que $a \equiv 0 \bmod m$. Alors a à le même reste que 0 dans la division euclidienne par m. Or $0 = m \times 0 + 0$ donc $r = 0$. Ainsi $a = mq$ donc a est un multiple de m.
- On suppose que a est un multiple de m. Alors il existe $k \in \mathbb{Z}$ tel que $a = mk$. Ainsi, $mk = a = mq + r$ d'où $r = m(k - q)$. Par suite, r est un entier naturel multiple de m et strictement inférieur à m ; donc $r = 0$. Il en résulte que $a \equiv 0 \bmod m$.

Proposition 3. *Transitivité*

Soit m un entier naturel non nul et a, b, c des entiers relatifs.
Si $a \equiv b \bmod m$ et $b \equiv c \bmod m$ alors $a \equiv c \bmod m$.

Démonstration.

On suppose $a \equiv b \bmod m$ et $b \equiv c \bmod m$. Montrons que $a \equiv c \bmod m$. Comme $a \equiv b \bmod m$ et $b \equiv c \bmod m$, a a le même reste que b dans la division euclidienne par m et b a le même reste que c dans la division euclidienne par m. Par suite, a a le même reste que c dans la division euclidienne par m. D'où $a \equiv c \bmod m$. □

Proposition 4. *Opérations sur les congruences*

Soit m un entier naturel non nul et a, b, c, d des entiers relatifs.
Si $a \equiv b \bmod m$ et $c \equiv d \bmod m$ alors :

- $a + c \equiv b + d \bmod m$;
- $ac \equiv bd \bmod m$;
- pour tout $n \in \mathbb{N}$, $a^n \equiv b^n \bmod m$.

Démonstration.

On suppose $a \equiv b \bmod m$ et $c \equiv d \bmod m$. D'après la proposition 2, comme $a \equiv b \bmod m$, $a - b$ est un multiple de m donc il existe $k \in \mathbb{Z}$ tel que $a - b = mk$; et comme $c \equiv d \bmod m$, $c - d$ est un multiple de m donc il existe $\ell \in \mathbb{Z}$ tel que $c - d = m\ell$.

- On a :
$$(a+c)-(b+d)=(a-b)+(c-d)=mk+m\ell=m\underbrace{(k+\ell)}_{\in\mathbb{Z}},$$
d'où $(a+c)-(b+d)$ est un multiple de m. Ainsi, d'après la proposition 2, $a+c\equiv b+d \bmod m$.
- On a :
$$(ac)-(bd)=ac-bc+bc-bd=(a-b)c+b(c-d)=mkc+bm\ell=m\underbrace{(ck+b\ell)}_{\in\mathbb{Z}},$$
d'où $(ac)-(bd)$ est un multiple de m. Ainsi, d'après la proposition 2, $ac\equiv bd \bmod m$.
- On raisonne par récurrence sur $n\in\mathbb{N}$ (A faire chez soi rigoureusement !).

□

Remarque 2.

Attention ! La réciproque des propriétés précédentes sont fausses en général :
Par exemple : $1+2\equiv 2+1 \bmod 4$ mais $1\not\equiv 2 \bmod 4$!

Conséquence : on ne peut PAS simplifier une congruence comme on le ferait avec une égalité :

$$na\equiv nb \bmod m \quad \not\Rightarrow \quad a\equiv b \bmod m$$
$$a^n\equiv b^n \bmod m \quad \not\Rightarrow \quad a\equiv b \bmod m$$

4. Exercices

Exercice 22.

1. Déterminer, pour tout $n\in\mathbb{N}^*$, le reste de la division euclidienne de 2^n par 6.
2. Déterminer le reste de la division euclidienne de 152^{403} par 6.

Exercice 23.

Déterminer le reste de la division euclidienne de 2023^{2023} par 5.

Exercices : Exercice 41,42 p127,128

Exercice 24.

Exercices 45 p128, 78p129, 88,89p132, 94p133