Chapitre 1 : Introduction à l'arithmétique

C. Aupérin

2009-2010

"Télécharger c'est tuer l'industrie, tuons les tous" Thurston Moore
Dernière modification : 8 octobre 2009

Table des matières

Cours : Introduction à l'arithmétique

1 Histoire

1.1 L'arithmétique

L'arithmétique constitue une grosse partie du programme de spécialité en terminale S. Son abord est facile, car le langage est simple et les objets définis ont déjà été abordés en classe de seconde. Cependant, cette partie des mathématiques est réputée difficile, car elle nécessite un temps d'adaptation avant d'en saisir les mécanismes et l'état d'esprit.

L'arithmétique c'est la théorie des nombres entiers, un des plus vieux domaines des mathématiques. Elle étudie les propriétés des nombres entiers (au départ seulement des naturels), de manière totalement abstraite et indépendamment de leur représentation écrite et des objets comptés.

En Occident, dès 600 avant JC, l'école pythagoricienne étudie déjà cette théorie, puisque sa philosophie est que tout est nombre et que tout nombre peut sécrire comme le quotient de deux entiers naturels. Evidemment ce fut un choc de constater que ce n'était pas le cas de la diagonale d'un carré de côté 1 (sans parler du fait que les nombres relatifs n'étaient pas encore connus) !

Euclide (environ 300 avant JC) fut le premier à donner les fondements de l'arithmétique, en résumant toutes les connaissances de l'époque dans trois volumes de ses *Éléments*. Mais son système de numération était différent du notre, le zéro n'a pas encore sa place en tant que nombre et il n'y avait toujours aucune connaissance des nombres relatifs. C'est donc bien plus tard, à partir 800 après JC jusqu'à nos jours, que l'arithmétique se développera réellement, grâce au système de numération positionnel et des chiffres.arabes, ainsi que par la nouvelle méthode de travail d'Al Khwarizmi, à savoir détacher les mathématiques de leur côté concret et surtout contextuel, pour les voir comme une théorie globale.

Au départ, l'arithmétique était donc considérée comme abstraite et sans autre réel utilité que pour sa beauté, contrairement aux autres branches des mathématiques, issues de la nécessité de résoudre des problèmes concrets et de comprendre le monde. On étudiait l'arithmétique pour former l'esprit humain à la réflexion ou pour le côté mystique parfois attribué aux nombres (comme pour les Pythagoriciens).

Cependant, l'arithmétique trouve aujourd'hui de nombreuses applications concrètes dans divers domaines, tels que la cryptographie (théorie de l'encodage et du décodage de messages secrets, qui utilise les propriétés des nombres premiers),les images numériques, la téléphonie cellulaire, ... De plus, la recherche de résolution de problèmes purement arithmétiques entraina la découverte et le développement d'outils et de méthodes très efficaces pour résoudre des problèmes plus concrets. L'arithmétique fut donc un facteur important de l'évolution de toutes les branches mathématiques.

1.2 Les nombres

L'ensemble des entiers naturels s'est construit de manière naturelle justement, empirique et non mathématiques (il n'y a d'ailleurs pas de défintion mathématiques satisfaisante de $\mathbb{N}$). Les entiers naturels dénombrent des objets, ce qui est vital dans une vie sociale, en groupe, d'où leur apparition dans le monde humain dès 35 000 avant notre ère au moins (sauf pour le zéro, car on ne voit alors encore aucune utilité de comptabiliser le vide et l'on ne pense pas pouvoir travailler avec le vide comme avec un nombre fini d'objets).

Les mathématiciens ont découvert peu à peu d'autres nombres, comme les quotients d'entiers positifs. Grâce au théorème de Pythagore, ils ont entrevu l'existence de quelques irrationnels ($\sqrt{2}$).

Ce n'est qu'avec l'apparition du zéro en tant que nombre à part entière (et non simplement comme place vide dans un système de numération positionnel) que la connaissance des nombres se développe vraiment. Rapidement, Al Kwharizmi décide de classer les équations et de les résoudre en dehors de tout contexte. Il est alors confronté à devoir faire la soustraction de n'importe quel entier naturel à un autre. La découverte des entiers relatifs en découle et donc de l'ensemble des rationnels.

Les ensembles de nombres sont construits de cette façon. A chaque fois que l'ensemble le plus vaste connu ne permet pas de faire telle ou telle opération, on en construit un plus grand. C'est ainsi que l'on construisit $\mathbb{R}$ à partir de $\mathbb{Q}$, en rajoutant les irrationnels . De même, à partir de $\mathbb{R}$, on construisit $\mathbb{C}$, l'ensemble des nombres complexes, dans lequel les racines de nombres négatifs existent. Le vocabulaire employé montre bien la distance prise par les mathétatiques depuis les entiers naturels.

2 Les nombres entiers

2.1 Les entiers naturels : $\mathbb{N}$

Définition 1. $\mathbb{N} = \{0; 1; 2; 3; 4; 5; 6; \dots\}$

Propriété 1. $\mathbb{N}$ est stable pour l'addition et la multiplication :

$$\forall x \in \mathbb{N}, \forall y \in \mathbb{N}, \text{ on a } x + y \in \mathbb{N} \text{ et } xy \in \mathbb{N}$$

Le mot « axiome »vient du grec et signifie « qui est considéré comme évident en soi »(et ne nécessite donc pas de preuve).

Axiome 1. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément. (Faux dans $\mathbb{Z}$)

Axiome 2. Toute partie non vide majorée de $\mathbb{N}$ admet un plus grand élément.

Axiome 3. Toute suite d'entiers naturels strictement décroissante est finie. (Faux dans $\mathbb{Z}$)

2.2 Les entiers relatifs : $\mathbb{Z}$

Définition 2. $\mathbb{Z} = \{\dots; -4; -3; -2; -1; 0; 1; 2; 3; 4; 5; 6; \dots\}$

Propriété 2. $\mathbb{Z}$ est stable pour l'addition, la soustraction et la multiplication :

$$\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, \text{ on a } x + y \in \mathbb{Z}, x - y \in \mathbb{Z} \text{ et } xy \in \mathbb{Z}$$

Propriété 3. Tout nombre de $\mathbb{Z}$ admet un opposé dans $\mathbb{Z}$:

$$\forall x \in \mathbb{Z}, \text{ on a } -x \in \mathbb{Z}$$

Propriété 4. $\mathbb{N} \subset \mathbb{Z}$:

$$\forall x \in \mathbb{N}, \text{ on a } x \in \mathbb{Z}$$

Axiome 4. Toute partie non vide majorée de $\mathbb{Z}$ admet un plus grand élément.

Contre-exemple : La partie constituée des nombres réels $2 - \frac{1}{x}$ avec $x \in \mathbb{R}^+$ est majorée par 2 mais n'admet pas de plus grand élément.

3 Divisibilité dans $\mathbb{Z}$

3.1 Multiples et diviseurs d'un entier relatif

Travail de l'élève : Math'x : Activité 1 p 4 ou 6 (Nombres croisés)
L'objectif est de réinvestir les notion de multiples, diviseur, nombre premier.

On note n et m deux entiers relatifs.

Définition 3. On dit que m est un multiple de n si et seulement si il existe un nombre entier relatif quelconque k tel que $m = k \times n$.

Exemples :
- Les multiples de 4 sont tous les nombres de la forme $4k$, avec $k \in \mathbb{Z}$. On note cet ensemble $4\mathbb{Z}$. Il est infini dénombrable.
- 0 est multiple de tout entier ($m = 0$ et il suffit de prendre $k = 0$ et alors $0 = 0 \times n$) mais il ne possède qu'un seul multiple, lui-même ($n = 0 \Rightarrow m = k \times 0 = 0$).

Définition 4. On suppose $n \neq 0$. On dit que n divise m (ou que n est un diviseur de m) si et seulement si il existe $k \in \mathbb{Z}$ tel que $m = k \times n$ (m est un multiple de n).
On note $n|m$ la relation n divise m.

Remarques :
- $\forall n \in \mathbb{Z}^*$, $1|n$ et $-1|n$ (on prend $k = \pm n$)
- $\forall n \in \mathbb{Z}^*$, $n|0$ (on prend $k = 0$, 0 admet une infinité de diviseurs)
- $\forall n \in \mathbb{Z}^*$, $n|n$ (on prend $k = 1$, on dit que la relation de divisibilité est réflexive)
- $\forall n \in \mathbb{Z}^*$, n admet au moins 4 diviseurs $\{-1; 1; n; -n\}$
- Tout nombre entier $n \neq 0$ admet un nombre fini de diviseurs, tous compris entre $-n$ et n (mais un nombre infini de multiples).

Définition 5. n et m sont premiers entre eux si et seulement si leurs seuls diviseurs communs sont 1 et -1.

Exemple : 6 et 35 sont premiers entre eux.

3.2 Propriétés de la division dans $\mathbb{Z}$.

Soient a, b et c trois entiers relatifs.

Propriété 5. $a|b \Rightarrow -a|b$

Démonstration :

(À faire par les élèves)
$a|b \iff \exists k \in \mathbb{Z}$ tel que $b = k \times a$. Donc $b = -k \times (-a)$ et $-k \in \mathbb{Z}$, d'où $-a|b$.

Propriété 6. $a|b$ et $b \neq 0 \Rightarrow |a| \leq |b|$

Démonstration :

(À faire par les élèves)
$a|b \iff \exists k \in \mathbb{Z}$ tel que $b = k \times a$. Donc $|b| = |k||a|$. Or $b \neq 0$ donc $k \in \mathbb{Z}^*$ et $|k| \geq 1$. D'où $|b| \geq |a|$.

Propriété 7. $a|b$ et $b|c \Rightarrow a|c$ (transitivité)

Démonstration :

(À faire par les élèves)
$a|b \iff \exists k_1 \in \mathbb{Z}$ tel que $b = k_1 \times a$.
$b|c \iff \exists k_2 \in \mathbb{Z}$ tel que $c = k_2 \times b$.
D'où $c = k_2 k_1 a$ avec $k_2 k_1 \in \mathbb{Z}$. Donc $a|c$.

Propriété 8. $a|b$ et $b|a \Rightarrow b = a$ ou $b = -a$

Démonstration :

(À faire par les élèves)
$a|b \Rightarrow |a| \leq |b|$.
$b|a \Rightarrow |b| \leq |a|$.
D'où $|a| = |b|$ et $a = \pm b$.

Propriété 9. Si $a|b$ et $a|c$ alors a divise toute combinaison linéaire de b et c.

$$a|b \text{ et } a|c \Rightarrow \forall (u;v) \in \mathbb{Z}^2 \quad a|(ub + vc)$$

Démonstration :

(À faire par les élèves)
$a|b \iff \exists k_1 \in \mathbb{Z}$ tel que $b = k_1 \times a$.
$a|c \iff \exists k_2 \in \mathbb{Z}$ tel que $c = k_2 \times a$.
Soit $(u; v) \in \mathbb{Z}^2$. Alors $ub + vc = u(k_1 a) + v(k_2 a) = (uk_1 + vk_2)a$ avec $(uk_1 + vk_2) \in \mathbb{Z}$ car $\mathbb{Z}$ est stable pour l'addition et la multiplication. Donc $a|(ub + vc)$.

Propriété 10. $a|b \Rightarrow \forall c \in \mathbb{Z} \quad a|bc$

Démonstration :

(À faire par les élèves)
$a|b \iff \exists k \in \mathbb{Z}$ tel que $b = k \times a$.
Alors $bc = (kc)a$ avec $kc \in \mathbb{Z}$ donc $a|bc$.

Propriété 11. $a|b \Rightarrow \forall c \in \mathbb{Z} \quad ac|bc$

Démonstration :

(À faire par les élèves)
$a|b \iff \exists k \in \mathbb{Z}$ tel que $b = k \times a$.
Alors $bc = k(ac)$ avec $k \in \mathbb{Z}$ donc $ac|bc$.

Application 1. Trouver les entiers n pour lesquels la fration $\dfrac{n+17}{n+4}$ est entière.

Application 2. Déterminer des entiers naturels a et b telsque $a^2 - 4b^2 = 20$.

4 Division euclidienne

4.1 Dans $\mathbb{N}$

Travail de l'élève : Math'x : Activité 2 p 5

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$ avec $a > b$.

THÉORÈME 1. Il existe un unique couple $(q;r)$ d'entiers naturels tels que $a = bq + r$ avec $0 \leq r < b$.
Dans ce cas, on dit que q est le quotient et r le reste de la division euclidienne de a par b.

Démonstration :

1. Existence du couple $(q;r)$:
   Elle repose sur le fait que $\mathbb{N}$ est archimédien : Soit $b \in \mathbb{N}^*$. Pour tout $a \in \mathbb{N}$, $\exists n \in \mathbb{N}$ tel que $a < nb$ (on peut rendre le produit nb aussi grand que l'on veut, pourvu que n soit suffisamment grand).
   Comme $\mathbb{N}$ est archimédien, l'ensemble des entiers naturels n tels que $a < nb$ n'est pas vide, donc il possède un plus petit élément, que l'on appellera k avec $k \neq 0$.
   On a $k-1 \in \mathbb{N}$ et $(k-1)b \leq a < kb$. On pose $q = k-1$ et on en déduit que $qb \leq a < (q+1)b$ et donc que $qb - qb \leq a - qb < qb + b - qb$ et on a bien $0 \leq a - qb < b$. On pose $r = a - qb$ et on a bien $a = qb + r$ avec $0 \leq r < b$.
2. Unicité du couple $(q;r)$:
   On raisonne par l'absurde : Supposons qu'il existe deux couples $(q_1;r_1)$ et $(q_2;r_2)$ tels que $a = bq_1 + r_1$ avec $0 \leq r_1 < b$ et $a = bq_2 + r_2$ avec $0 \leq r_2 < b$.
   Alors $r_2 - r_1 = b(q_2 - q_1)$ et $-b < r_2 - r_1 < b$.
   Donc $r_2 - r_1$ est un multiple de b strictement compris entre $-b$ et b. On en déduit $r_2 - r_1 = 0$ et donc $r_2 = r_1$.
   Si $r_2 = r_1$ alors $q_2 = q_1$ et les couples sont identiques.

Exemple : $17 = 3 \times 5 + 2$ donc 5 est le quotient et 2 le reste de la division euclidienne de 17 par 3.
Contre-exemple : $58 = 17 \times 2 + 24$ ne traduit pas la division euclidienne de 58 par 17 car $24 > 17$.

Remarque : $r = 0$ si et seulement si b divise a.

4.2 Dans $\mathbb{Z}$

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$ avec $a > b$.

THÉORÈME 2. Il existe un unique couple $(q;r)$ d'entiers relatifs tels que $a = bq + r$ avec $0 \leq r < |b|$.
Dans ce cas, on dit que q est le quotient et r le reste de la division euclidienne de a par b.

Démonstration :

1. Existence du couple $(q;r)$:
   L'ensemble des entiers naturels n tels que $a+|b|n \geq 0$ n'est pas vide. En effet, sinon la suite $(a+|b|k)_{k\in\mathbb{N}}$ serait strictement croissante et incluse dans $\mathbb{Z}^-$ donc aurait un plus grand élément (cf Axiome 1), ce qui est impossible.
   Le nombre $a+|b|n$ est dans $\mathbb{N}$, donc d'après ce qui précède, il existe un unique couple $(q';r')$ tel que $a+|b|n = |b|q'+r'$ avec $0 \leq r' < |b|$.
   Donc $a = |b|(q'-n)+r' = b\dfrac{|b|}{b}(q'-n)+r' = bq+r$ avec $q = \dfrac{|b|}{b}(q'-n)$ et $r = r'$
2. Unicité du couple $(q;r)$:
   On raisonne par l'absurde : Supposons qu'il existe deux couples $(q_1;r_1)$ et $(q_2;r_2)$ tels que $a = bq_1+r_1$ avec $0 \leq r_1 < |b|$ et $a = bq_2+r_2$ avec $0 \leq r_2 < |b|$.
   Alors $r_2 - r_1 = b(q_2-q_1)$ et $-|b| < r_2 - r_1 < |b|$.
   Donc $r_2 - r_1$ est un multiple de b strictement compris entre $-|b|$ et $|b|$. On en déduit $r_2 - r_1 = 0$ et donc $r_2 = r_1$.
   Si $r_2 = r_1$ alors $q_2 = q_1$ et les couples sont identiques.

Exemples : $-38 = 5\times(-8)+2$ donc 5 est le quotient et 2 le reste de la division euclidienne de -38 par -8.
$-126 = -7\times 19+7$ donc -7 est le quotient et 7 le reste de la division euclidienne de -126 par 19.

Remarque : r est toujours positif.

4.3 Application aux systèmes de numération

Un système de numération est un procédé qui permet d'écrire les entiers avec un certain nombre de symboles, appelés chiffres.

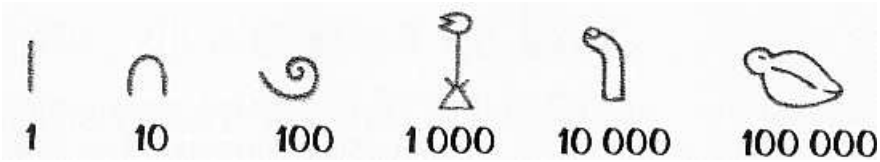
Presque toutes les civilisations anciennes ont trouvé des systèmes de numération. Cependant, il était souvent difficile de faire des opérations avec (rappelez-vous du système romain).

Les plus intéressants de ce point de vue furent, dans l'ordre chronologique, celui des Babyloniens, des Chinois et des Indiens. C'est d'ailleurs une variante de ce dernier que nous utilisons aujourd'hui, transmis par les arabes en Occident à partir d'environ 700, accepté par l'église uniquement vers 1300, sous la pression des marchands, pour qui les calculs étaient primordiaux.

Exemples :

1. **Le système Babyloniens** (2000 av JC)
   Les Babyloniens, environ 2000 ans avant JC, comptaient avec leurs phalanges jusqu'à 60. Pour écrire les nombres, ils gravaient des plaques d'argile à l'aide de roseaux. Au départ, ils utilisaient deux symboles (chiffres) : le clou T pour l'unité et le chevron < pour la dizaine.
   Pour représenter de grands nombres, ils adoptèrent une numération de position. Par exemple, 75 s'écrivait : T <TTTTT.
   Mais leur système ne comportait aucun sympbole pour zéro. Il était alors difficile de distinguer 18 de 180 et de 108. Il fallut attendre le VI^e s avant JC pour qu'apparaisse un symbole de position du zéro, mais zéro n'avait toujours pas le statu de nombre. Ce système en base 60 a survécu jusqu'à aujourd'hui dans notre façon de mesurer le temps et les angles. Les babyloniens furent entre autres prolifiques en conception de tables mathématiques (inverse, carrés, cubes, racines ...) grâce à ce système.

2. **Le système Égyptien** (1800 av JC)
   La civilisation égyptienne n'a laissé que peu témoignages mathématiques (le papyrus est un matériau très fragile). On sait cependant que les égyptiens utilisaient un système de numération additive avec un symbole particulier pour chaque puissance de 10.



   Les égyptiens savaient facilement multiplier un nombre par 2 et cela leur permettait de multiplier « rapidement »deux entiers entre eux.
   Par exemple pour faire 29×37, ils utilisaient le fait que $29 = 16 + 8 + 4 + 1 = 2^4 + 2^3 + 2^2 + 1$, ils développaient le produit et ils n'effectuaient que des additions et multiplications par 2.
   - Ecrire 345 puis 1789 en numération égyptienne.
   - Pourquoi ce système est-il qualifié d'*additif non positionnel à base 10* ?
   - Effectuer les multiplications 9×5 et 43×55.

3. **Le système binaire**
   Les ordinateurs utilisent le système positionnel binaire, grâce à l'algèbre de Boole (vient de Georges Boole, XIX^e). C'est la partie des mathématiques, de la logique et de l'électronique qui s'intéresse aux opérations sur les variables logiques. Elle permet de traduit des signaux (tout ou rien) en expressions mathématiques en remplaçant chaque signal élémentaire par des variables logiques et leur traitement par des suites d'opérations logiques. L'ordinateur peut avoir deux état logiques, pouvant prendre la valeur 0 ou 1.

4. Aujourd'hui, nous utilisons un système positionnel en base 10.
   Travail de l'élève : Math'x : TP 3 p 18

Notre système est dit **décimal** ou en base dix, car il permet d'écrire tous les nombres entiers en utilisant dix chiffres. Chaque nombre est décomposé en une somme de puissances de 10. Dans la numération de **position**, la valeur d'un chiffre varie suivant sa place, on parle de poids.

$$x = a_n.10^n + a_{n-1}.10^{n-1} + \cdots + a_1.10 + a_0$$

Exemple : $7325 = 7 \times 1000 + 3 \times 100 + 2 \times 10 + 5 \times 1 = 7 \times 10^3 + 3 \times 10^2 + 2 \times 10^1 + 5 \times 10^0$

Remarque : Cette numération présente des avantages :
- On peut facilement compter avec sur ses doigts.
- Son ordre de grandeur est satisfaisant
- Les normes internationales sont désormais construites sur cette base.

Mais elle possède également des inconvénients :
- 10 n'a que deux diviseurs
- 10 n'est pas premier ce qui ne permet pas décrire aisément les nombres à virgule sous forme de fraction irréductible
- Une puissance de 2 serait aujourd'hui adaptée à l'informatique

On peut écrire sur ce principe un nombre en n'importe quel base $b \geq 2$. Dans ce cas, les chiffres utilisés seront tous inférieurs strictement à b. Par exemple, on peut écrire :

$$x = b_m.2^m + b_{m-1}.2^{m-1} + \cdots + b_1.2 + b_0 \quad \text{le nombre } x \text{ en base 2, avec } b_i = 0 \text{ ou } 1$$

On note $\overline{b_m b_{m-1} \dots b_1 b_0}^2$ le nombre x en base 2.

Pour convertir un nombre en base b en un nombre décimal, il suffit de multiplier la valeur de chaque chiffre par son poids, puis additionner chaque résultat.

Exemple : $\overline{10111}^2 = 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 16 + 0 + 4 + 2 + 1 = 23$

Pour convertir un nombre décimal en base b, on utilise la division euclidienne par b.

Exemple : 37. On sait que ce nombre peut se décomposer ainsi :

$$37 = ...a_3 \times 2^3 + a_2 \times 2^2 + a_1 \times 2^1 + a_0 \times 2^0 = 2\left(...a_3 \times 2^2 + a_2 \times 2^1 + a_1 \times 2^0\right) + a_0$$

Donc si l'on efectue la division euclidienne de 37 par 2, le reste sera a_0.
Sur le même principe, en divisant le quotient obtenu

$$...a_3 \times 2^2 + a_2 \times 2^1 + a_1 \times 2^0 = 2 \times ..a_3 \times 2^1 + a_2 \times 2^0) + a_1$$

par 2, le reste sera a_1, et ainsi de suite, jusqu'à ce que le quotient soit nul.

$$\begin{aligned} 37 &= 18 \times 2 + \underline{1} \\ 18 &= 9 \times 2 + \underline{0} \quad \text{Poser les divsions successives pour plus de clarté} \\ 9 &= 4 \times 2 + \underline{1} \\ 4 &= 2 \times 2 + \underline{0} \\ 2 &= 1 \times 2 + \underline{0} \\ 1 &= 0 \times 2 + \underline{1} \end{aligned}$$

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

Exemples :

1. Écrire 234 en base 2. Pour cela, on utilisera la division euclidienne de 234 par 2.
2. Écrire tous les chiffres de la numération décimale en base 2.
3. Quels sont les eniters définis par : $\overline{14}^9$? $\overline{14}^5$? $\overline{14}^2$? $\overline{421}^6$?
4. Écrire 234 en base 5, puis en base 16.

Remarque : Le principe est le même pour passer d'une base N à une base M. La difficulté est cependant d'effectuer les divisions euclidiennes en base N. On préfèrera plutôt passer par l'intermédiaire de la base 10, ie transformer le nombre de base N en base 10 (avec les poids affectés à chaque chiffre) puis en base M (en effectuant des divisions euclidiennes successives du nombre par M.

Exercice 1.

1. Soit $n = 2183$ dans le système décimal. Déterminer son écriture en base 8.
2. Soit lenombre 5241, écrit dans une certaine base.
   - Peut-il être écrit e base 5 ?
   - Supposons qu'il soit écrit en base 6. Donner sa correspondance en base 10.

Exercice 2. Ecrire l'ensemble de tous les diviseurs dans $\mathbb{Z}$ de chacun des nombres 20, 28 et 75.

Exercice 3. a et b sont des entiers avec $b \neq 0$.
A quelle condition le nombre $\frac{a}{b}$ est-il entier ?

Exercice 4. Soit un entier a quelconque. Prouver que $a(a^2 - 1)$ est un multiple de 6.

Exercices du livre Math'x : 9-11 ? 12 - 13 ? 15 - 17 - 18 - 19... p 24 et 89 à 93

Exercice 5. Questions classiques (indépendantes)

1. Soit n un entier relatif. En vérifiant que $2n + 1 = 2(n - 3) + 7$ trouver l'ensemble des entiers n telsque $(n - 3)$ divise $(2n + 1)$.
2. Soit n un entier naturel. En vérifiant que $n^2 - n + 3 = (n - 2)(n + 1) + 5$ trouver l'ensemble des entiers n telsque $(n + 1)$ divise $(n^2 - n + 3)$.
3. Déterminer les valeursdel'entier relatifs n pour lesquelles la fraction $\frac{3n + 8}{n + 4}$ peut se simplifier sous forme d'un entier relatif.

Exercice 6. $n \in \mathbb{N}$ tel que $n \geq 2$ et $A = n^4 - 1$.

1. Démontrer que $n - 1$, $n + 1$, $n^2 + 1$ sont des diviseurs de A.
2. En déduire d'autres diviseurs de A.

Exercice 7.

1. Trouver tous les diviseurs dans $\mathbb{N}$ de 21.
2. Trouver tous les couples $(a; b)$ d'entiers naturels tels que $a^2 - b^2 = 21$

Exercice 8. Trouver tous les couples d'entiers naturels $(x; y)$ tels que $x^2 - 2xy = 15$

Exercice 9. Soient k un entier naturel, $a = 9k + 2$ et $b = 12k + 1$.
Prouver que les seuls diviseurs positifs communs aux entiers a et b sont 1 et 5.
Utiliser la propriété 5 avec des valeurs de u et v bien choisies.

Exercice 10. Soient k un entier naturel, $a = 6k + 5$ et $b = 8k + 3$.
Prouver que les seuls diviseurs positifs communs aux entiers a et b sont 1 et 11.

Exercice 11. Soient k un entier naturel, $a = 3k + 5$ et $b = 2k + 1$.
Prouver que les seuls diviseurs positifs communs aux entiers a et b sont 1 et 7.

Exercice 12. Trouver tous les entiers naturels n tels que $n + 8$ est un mutiple de n.

Exercice 13. Expliquer pourquoi il est impossible de trouver u et v dans $\mathbb{Z}$ tels que $6v - 9v = 2$.

Exercice 14. Déterminer selon les valeurs de l'entier naturel n le reste de la division euclidienne de $n^2 + 5n + 9$ par $n + 2$.

Exercice 15. Problème de bac

1. Démontrer que $n^2 + 5n + 4$ et $n^2 + 3n + 2$ sont divisibles par $n + 1$
2. Déterminer l'ensemble des valeurs de n pour lesquelles $3n^2 + 15n + 19$ est divisible par $n + 1$
3. En déduire que pour tout n,$3n^2 + 15n + 19$ n'est pas divisible par $n^2 + 3n + 2$

Exercice 16. Soit $n \in \mathbb{N}$. Démontrer que quel que soit n,$3n^2+5n+1$ est impair ; puis que ce polynôme n'est jamais divisible par $n(n + 1)$.

Exercices du livre 28 - 29 - 30 - 33 - 34 p 23 + 41 - 42 - 43 - 48 - 49 - 50 - 51 p 24

5 Congruence dans $\mathbb{Z}$

Travail de l'élève : On numérote les 365 jours de l'année 2009 de 1 à 365 de manière à pouvoir désigner chaque jour de l'année par son numéro. Le 1^{er} janvier 2009 était un jeudi.

1. (a) Quelle est la forme générale du numéro d'un jeudi quelconque de l'année ?
   (b) Parmi les jours de numéros 141, 153, 179, 343, quels sont ceux qui tombent un jeudi ?
2. Comment peut-on reconnaître qu'un jour dont le numéro est n est tombé un vendredi ? un samedi ?
3. Les jours $n = 145$ et $p = 292$ tombent-ils un même jours de la semaine ?
4. Quel jour de la semaine fut le 14 juillet 2009 ? 1789 ? *(Compter le nombre de jours écoulé entre ces deux dates)*

Définition 6. On note $n \geq 2$ un entier naturel et a et b deux entiers relatifs.
On dit que a et b sont congrus modulo n et on note $a \equiv b\,[n]$ si les divisions euclidiennes de a et b par n ont le même reste.

Exemples : $33 \equiv 13\,[5]$, $29 \equiv -121\,[5]$ et $-623 \equiv 17\,[10]$

On note n et n' deux entiers naturels tels que $n \geq 2$ et $n' \geq 2$. On note a, b et c trois entiers relatifs.
Remarque : Les nombres congrus à a modulo n sont tous les nombres de la forme $a + kn$ avec $k \in \mathbb{Z}$.

Propriété 12. Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$ alors $a \equiv c\,[n]$

Démonstration :

Découle de la définition.

Propriété 13.

$$a \equiv b\,[n] \iff n|(a-b)$$

Démonstration :

$\Rightarrow$: Si $a \equiv b\,[n]$ alors il existe un unique couple (q, r) d'entiers tel que $a = qn + r$ avec $0 \leq r < n$ et un unique couple (q', r) d'entiers tels que $b = q'n + r$.
Donc $a - b = qn - q'n = (q - q')n$ et $n|(a - b)$

$\Leftarrow$: Si $n|(a - b)$ alors il existe $k \in \mathbb{N}$ tel que $a - b = kn$.
D'après la division euclidienne, il existe un unique couple (q, r) avec $0 \leq r < n$ tel que $a = qn + r$ et un unique couple (q', r') avec $0 \leq r' < n$ tel que $b = q'n + r'$.
Donc $a - b = (q - q')n + r - r'$ avec $-n < r - r' < n$. Comme $a - b$ est un multiple de n on a $r - r'$ est un multiple de n.
Or $r - r' \in \mathbb{N}$ et le seul multiple de n dans $]-n; n[$ est 0. Donc $r = r'$ et $a \equiv b\,[n]$

Propriété 14. $a \equiv 0\,[n] \iff n|a$

Démonstration :

Cas particulier de la propriété précédente avec $b = 0$

Propriété 15. Si $n'|n$ alors $a \equiv b\,[n] \Rightarrow a \equiv b\,[n']$

Démonstration :

Si $n'|n$ alors il existe $k \in \mathbb{N}$ tel que $n = kn'$. Alors :
$a \equiv b\,[n] \iff$ il existe $p \in \mathbb{N}$ tel que $a = b + np$. Donc $a = b + n'kp = b + (kp)n'$.
Or $kp \in \mathbb{N}$ donc $a \equiv b\,[n']$

THÉORÈME 3. On note a, a', b et b' quatre entiers relatifs quelconques et $n \geq 2$ un entier naturel. Si $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$ alors :

$$a + b \equiv a' + b'\,[n]$$
$$a - b \equiv a' - b'\,[n]$$
$$ab \equiv a'b'\,[n]$$
$$\forall k \in \mathbb{Z}, \quad ka \equiv ka'\,[n]$$
$$\forall p \in \mathbb{N} a^p \equiv a'^p\,[n]$$

Attention !!. $ka \equiv ka'\,[n] \not\Rightarrow a \equiv a'\,[n]$

Contre-exemple : $16 \equiv 20\,[4]$ mais 8 et 10 ne sont pas congrus modulo 4

Démonstration :

Si $a \equiv a'\,[n]$ il existe $k_1 \in \mathbb{N}$ tel que $a = a' + k_1 n$ Si $b \equiv b'\,[n]$ il existe $k_2 \in \mathbb{N}$ tel que $b = b' + k_2 n$
Donc :

$$a + b = (a' + b') + n(k_1 + k_2) \quad \text{Donc } a + b \equiv a' + b'\,[n]$$
$$a - b = (a' - b') + n(k_1 - k_2) \quad \text{Donc } a - b \equiv a' - b'\,[n]$$
$$ab = (a' + k_1 n)(b' + k_2 n) = a'b' + n(a'k_2 + b'k_1 + k_1 k_2 n) \quad \text{Donc } ab \equiv a'b'\,[n]$$
$$\forall k \in \mathbb{Z}, \quad ka = ka' + nk_1 \quad \text{Donc } ka \equiv ka'\,[n]$$

On démontre cette partie par récurrence :
Initialisation : On a $a^1 \equiv a'^1\,[n]$
Hérédité : On suppose que la propriété est vraie au rang k, donc que $a^k \equiv a'^k\,[n]$
Alors $a^{k+1} = a^k \times a \equiv a'^k\,[n]$. Donc $a^{k+1} \equiv a'^{k+1}\,[n]$.
La propriété est héréditaire et vraie au rang 1. Elle est vraie pour tout $p \in \mathbb{N}^*$

Exercices du livre Transmath : TP 1-2 p 16

Exercice 17. Démontrer que $2^{3n} - 1$ est divisible par 7 pour tout $n \in \mathbb{N}$.

Exercice 18. Démontrer que $671^{800} - 1$ est divisible par 6.

Exercice 19. Le but de cet exercice est de calcuer lereste de la division par 7 du nombre 247^{349}

1. Vérifier que $247 \equiv 2\,[7]$
2. Vérifier que $2^{3k} \equiv 1$, $2^{3k+1} \equiv 2$,$2^{3k+2} \equiv 4$ [7]
3. En déduire le reste de la division de 247^{349} par 7.

Les Annexes

Exercices

Exercice 1.

1. Soit $n = 2183$ dans le système décimal. Déterminer son écriture en base 8.
2. Soit le nombre 5241, écrit dans une certaine base.
   - Peut-il être écrit en base 5 ?
   - Supposons qu'il soit écrit en base 6. Donner sa correspondance en base 10.

Exercice 2. Ecrire l'ensemble de tous les diviseurs dans $\mathbb{Z}$ de chacun des nombres 20, 28 et 75.

Exercice 3. a et b sont des entiers avec $b \neq 0$.
A quelle condition le nombre $\dfrac{a}{b}$ est-il entier ?

Exercice 4. Soit un entier a quelconque. Prouver que $a(a^2 - 1)$ est un multiple de 6.

Exercice 5. Questions classiques (indépendantes)

1. Soit n un entier relatif. En vérifiant que $2n + 1 = 2(n - 3) + 7$ trouver l'ensemble des entiers n telsque $(n - 3)$ divise $(2n + 1)$.
2. Soit n un entier naturel. En vérifiant que $n^2 - n + 3 = (n - 2)(n + 1) + 5$ trouver l'ensemble des entiers n telsque $(n + 1)$ divise $(n^2 - n + 3)$.
3. Déterminer les valeurs de l'entier relatifs n pour lesquelles la fraction $\dfrac{3n + 8}{n + 4}$ peut se simplifier sous forme d'un entier relatif.

Exercice 6. $n \in \mathbb{N}$ tel que $n \geq 2$ et $A = n^4 - 1$.

1. Démontrer que $n - 1$, $n + 1$, $n^2 + 1$ sont des diviseurs de A.
2. En déduire d'autres diviseurs de A.

Exercice 7.

1. Trouver tous les diviseurs dans $\mathbb{N}$ de 21.
2. Trouver tous les couples $(a; b)$ d'entiers naturels tels que $a^2 - b^2 = 21$

Exercice 8. Trouver tous les couples d'entiers naturels $(x; y)$ tels que $x^2 - 2xy = 15$

Exercice 9. Soient k un entier naturel, $a = 9k + 2$ et $b = 12k + 1$.
Prouver que les seuls diviseurs positifs communs aux entiers a et b sont 1 et 5.
Utiliser la propriété 5 avec des valeurs de u et v bien choisies.

Exercice 10. Soient k un entier naturel, $a = 6k + 5$ et $b = 8k + 3$.
Prouver que les seuls diviseurs positifs communs aux entiers a et b sont 1 et 11.

Exercice 11. Soient k un entier naturel, $a = 3k + 5$ et $b = 2k + 1$.
Prouver que les seuls diviseurs positifs communs aux entiers a et b sont 1 et 7.

Exercice 12. Trouver tous les entiers naturels n tels que $n + 8$ est un mutiple de n.

Exercice 13. Expliquer pourquoi il est impossible de trouver u et v dans $\mathbb{Z}$ tels que $6v - 9v = 2$.

Exercice 14. Déterminer selon les valeurs de l'entier naturel n le reste de la division euclidienne de $n^2 + 5n + 9$ par $n + 2$.

Exercice 15. Problème de bac

1. Démontrer que $n^2 + 5n + 4$ et $n^2 + 3n + 2$ sont divisibles par $n + 1$
2. Déterminer l'ensemble des valeurs de n pour lesquelles $3n^2 + 15n + 19$ est divisible par $n + 1$
3. En déduire que pour tout n,$3n^2 + 15n + 19$ n'est pas divisible par $n^2 + 3n + 2$

Exercice 16. Soit $n \in \mathbb{N}$. Démontrer que quel que soit n, $3n^4+5n+1$ est impair ; puis que ce polynôme n'est jamais divisible par $n(n + 1)$.

Exercice 17. Démontrer que $671^{800} - 1$ est divisible par 6.

Exercice 18. Le but de cet exercice est de calculer lereste de la division par 7 du nombre 247^{349}

1. Vérifier que $247 \equiv 2\,[7]$
2. Vérifier que $2^{3k} \equiv 1$, $2^{3k+1} \equiv 2$,$2^{3k+2} \equiv 4$ $[7]$
3. En déduire le reste de la division de 247^{349} par 7.

Exercice de spécialité : *Les questions sont indépendantes.*

1. Pour quelles valeurs de l'entier relatif m la fraction $\dfrac{2m-5}{m+8}$ est-elle elle-même un entier ?
2. k étant un entier relatif, on pose : $x = 2k - 1$ et $y = 9k + 4$.
   Montrer que tout diviseur commun à x et à y divise 17.
3. Déterminer les entiers naturels u et v vérifiant la relation : $u^2 - 4v^2 = 12$
4. n est un entier naturel. Démontrer que quel que soit n, $3n^2 + 5n + 1$ est impair .
   En déduire que ce nombre n'est jamais divisible par $n(n+1)$.

Exercice de spécialité : *Les questions sont indépendantes.*

1. Pour quelles valeurs de l'entier relatif m la fraction $\dfrac{2m-5}{m+8}$ est-elle elle-même un entier ?
2. k étant un entier relatif, on pose : $x = 2k - 1$ et $y = 9k + 4$.
   Montrer que tout diviseur commun à x et à y divise 17.
3. Déterminer les entiers naturels u et v vérifiant la relation : $u^2 - 4v^2 = 12$
4. n est un entier naturel. Démontrer que quel que soit n, $3n^2 + 5n + 1$ est impair .
   En déduire que ce nombre n'est jamais divisible par $n(n+1)$.

Correction Exercice de spécialité :

1. $\dfrac{2m-5}{m+8} = \dfrac{2m+16-21}{m+8} = 2 - \dfrac{21}{m+8}$.

   Donc $m + 8$ doit diviser 21. Les diviseurs de 21 sont 1, 3, 7, et 21 et leurs opposés.
   Les valeurs de m possibles sont alors :
   $m = -7$, $m = -5$, $m = -1$, $m = 13$ et $m = -9$, $m = -11$, $m = -15$ et $m = -29$

2. Soit d un diviseur commun à x et y. Alors d divise toute combinaison linéaire de x et y.
   En particulier, d divise $-9x + 2y = -18k + 9 + 18k + 8 = 17$ donc d divise 17.

3. Les diviseurs naturels de 12 sont 1, 2, 3, 4, 6 et 12.
   Or $u^2 - 4v^2 = (u - 2v)(u + 2v)$ et u et v étant naturels on a $u - 2v \leq u + 2v$

   Donc on doit avoir $\begin{cases} u-2v=1 \\ u+2v=12 \end{cases}$ ou $\begin{cases} u-2v=2 \\ u+2v=6 \end{cases}$ ou $\begin{cases} u-2v=3 \\ u+2v=4 \end{cases}$

   Le seul système ayant des solutions naturelles est le deuxième. On trouve $u = 4$ et $v = 1$.

4. – Si n est pair, alors il existe $p \in \mathbb{N}$ tel que $n = 2p$ et
   $3n^2 + 5n + 1 = 3 \times 4p^2 + 10p + 1 = 2(6p^2 + 5p) + 1$.
   Le nombre considéré est donc impair.

   – Si n est impair, alors il existe $p \in \mathbb{N}$ tel que $n = 2p + 1$ et
   $3n^2 + 5n + 1 = 3(4p^2 + 4p + 1) + 10p + 5 + 1 = 12p^2 + 12p + 3 + 10p + 6 = 2(6p^2 + 11p + 4) + 1$.
   Le nombre considéré est donc impair.

   – Or $n(n + 1)$ est toujours pair (car soit n l'est, soit $(n + 1)$).
   Donc si $n(n + 1)$ divise $3n^2 + 5n + 1$, alors 2 divise un nombre impair, ce qui est absurde.

Devoir Maison 1

Exercice 1. n°61 p 28 : $u_n = 3^{2n+1} + 2^{n+2}$

1. $u_0 = 3^1 + 2^2 = 7 = 7 \times 1$,
   $u_1 = 3^3 + 2^3 = 27 + 8 = 35 = 7 \times 5$,
   $u_2 = 3^5 + 2^4 = 243 + 16 = 259 = 7 \times 37$,
   $u_3 = 3^7 + 2^5 = 2187 + 32 = 2219 = 7 \times 317$,
   $u_4 = 3^9 + 2^6 = 19683 + 64 = 19747 = 7 \times 2821$,
   $u_5 = 3^{11} + 2^7 = 177147 + 128 = 177275 = 7 \times 25325$,

2.
$$\begin{aligned} u_{n+1} &= 3^{2(n+1)+1} + 2^{n+1+2} \\ &= 3^{2n+3} + 2^{n+3} \\ &= 9 \times 3^{2n+1} + 2 \times 2^{n+1} \\ &= 7 \times 3^{2n+1} + 2 \times 3^{2n+1} + 2 \times 2^{n+1} \\ &= 7 \times 3^{2n+1} + 2u_n \end{aligned}$$

3. – **Initialisation** : on a déj'a montrer que u_0 est divisible par 7.

   – **Hérédité** : Supposons qu'il existe $k \in \mathbb{N}$ tel que u_k est divisble par 7, montrons que u_{k+1} est divisible par 7.
   u_k est divisble par 7 donc il existe $p \in \mathbb{N}$ tel que $u_k = 7p$.
   Or $u_{k+1} = 7 \times 3^{2k+1} + 2u_k = 7 \times 3^{2k+1} + 2 \times 7p = 7(3^{2k+1} + 2p)$.
   Et $3^{2k+1} + 2p \in \mathbb{N}$. Donc u_{k+1} est divisible par 7.

   – La propriété est vraie au rang 0 et est héréditaire. Donc elle est vraie pour tout $n \in \mathbb{N}$

Exercice 2. n°75 p 29 :

1. Soit d un diviseur commun à x et y. Alors d divise toute combinaison linéaire de x et y. Par exemple, $x + y = A$ et $2x + 3y = B$. Donc d divise A et B.

2. $\left\{ \begin{array}{l} A = x + y \\ B = 2x + 3y \end{array} \right. \iff \left\{ \begin{array}{l} x = A - y \\ B = 2(A - y) + 3y \end{array} \right. \iff \left\{ \begin{array}{l} x = A - y \\ B = 2A + y \end{array} \right. \iff \left\{ \begin{array}{l} y = B - 2A \\ x = A - B + 2A \end{array} \right.$
   $\iff \left\{ \begin{array}{l} y = B - 2A \\ x = 3A - B \end{array} \right.$

   Et tout diviseur commun à A et B divise toute combinaison linéaire de A et B, par exemple, x et y.

3. On pose $x = 2^n$ et $y = 3^n$. Alors $2^n + 3^n = x + y = A$ et $2^{n+1} + 3^{n+1} = 2x + 3y = B$.
   Alors tout diviseur commun à A et B divise 2^n et 3^n. Mais 2^n et 3^n sont clairement premiers entre eux.
   Donc les diviseurs communs de A et B sont forcément 1 ou -1 et A et B sont premiers entre eux.

Exercice 3. n°78 p 29 :

1. Si le diviseur est 2, alors le reste est $3 > 2$ donc la division n'est pas euclidienne.
   Sinon, on doit avoir $2^n - 1 > 3 \iff 2^n > 4 \iff n > 2$.

2. Si le diviseur est n, alors on doit avoir $n > 4$ pour que la division soit euclidienne.
   Sinon, le diviseur est $n - 4$ et on doit avoir $n - 4 > 4 \iff n > 8$.

3. Si le diviseur est 3, alors on a $3 > 1$ donc la division est euclidienne.
   Sinon, le diviseur est $3n^2 + 2n$ mais ceci vaut 0 quand $n = 0$, ce qui est interdit.

   Au final, on peut dire que seule la dernière est une division euclidienne pour tout $n \in \mathbb{N}$

Exercice 4. n°28 p 29 :

On a $\begin{cases} m = bq + r \\ m + 5 = b(q+3) + r - 1 \end{cases} \iff \begin{cases} m = bq + r \\ 5 = 3b - 1 \quad (L_2 - L_1) \end{cases} \iff \begin{cases} b = 2 \\ m = 2q + r \end{cases}$

Donc, on sait que $r = 0$ ou $r = 1$ car $0 \leq r < b$. Mais on a aussi $0 \leq r - 1 < b$. Donc $r = 1$.
Alors $m = 2q + 1$ et $m + 5 = 2q + 6$, mais ces égalités sont équivalentes et l'on a pas d'autres conditions sur m.
Finalement, il suffit que m soit impair.