Chapitre 2
Arithmétique : Divisibilité & Congruence

Sommaire

Capacités :	Exercices :	Bilan :				
Déterminer les diviseurs d'un entier	1 et 2 p. 126					
Utiliser les combinaisons linéaires pour étudier la divisibilité	8 et 17 p. 126					
Effectuer une division euclidienne	19, 21 et 30 p. 126/127					
Calculer avec les congruences	33, 34 et 36 p. 127					
Utiliser les congruences pour des problèmes d'arithmétique	38 et 40 p. 127					

ERATOSTHENE ($\approx$ 276 av. J.C. - $\approx$ 194 av. J.C.) est un mathématicien grec qui séjourne à Athènes et acquiert une grande notoriété. Il est nommé directeur de la bibliothèque d'Alexandrie.
Il est notamment connu pour sa méthode de recherche des nombres premiers ainsi que sa mesure du périmètre de la Terre.
Doué intellectuellement, il est également un athlète confirmé. Ses élèves l'appellent β en référence à la seconde lettre de l'alphabet grec et ses résultats sportifs.

Introduction

L'arithmétique concerne l'étude des entiers naturels ($\mathbb{N} = \{0; 1; 2; \dots\}$) ou relatifs ($\mathbb{Z} = \{\dots; -2; -1; 0; 1; 2; 3 \dots\}$).

- Les entiers naturels : $\mathbb{N}$.

  L'ensemble des entiers naturels s'est construit de façon tout à fait "naturelle". Ce nom qui lui a été attribué, provient du fait qu'ils remplissaient à l'origine la fonction fondamentale des mathématiques : le dénombrement d'objets. Les besoins des Hommes, dès lors que l'on vit en société, sont et doivent être quantifiés : ne serait-ce par exemple que la nourriture ! Le dénombrement des ressources est une fonction vitale pour la survie du groupe.

  En cela, l'ensemble des entiers naturels ne s'est pas construit de façon mathématique mais de façon empirique (expérimental/déductif), lorsque l'Homme a dû quantifier et compter les éléments nécessaires à son existence. Toutefois cet ensemble $\mathbb{N}$, ne permet alors que de sommer des quantités : la soustraction est impossible (pas d'existence de symétrique à 2 ; 3 ; ...). Cet ensemble devient donc vite insuffisant lorsque les besoins (et le cerveau) de l'Homme évoluent : on ne s'occupe plus que de dénombrer, mais établir des lois entre ces quantités dénombrables. L'ensemble des naturels ne répond pas à cette attente, c'est pour cela qu'un nouvel ensemble plus vaste et permettant plus d'opérations va être créé : l'ensemble des entiers relatifs $\mathbb{Z}$.

  La création de cet ensemble va permettre de pouvoir additionner et soustraire toutes les quantités que l'on voudrait, ce qui était impossible dans $\mathbb{N}$.

- Les entiers relatifs : $\mathbb{Z}$.

  L'ensemble des entiers relatifs est obtenu en rajoutant tous les symétriques des nombres entiers naturels pour la soustraction (c'est-à-dire les opposés).

  L'ensemble $\mathbb{Z}^+$ désigne l'ensemble des entiers relatifs positifs, c'est-à-dire $\mathbb{Z}^+ = \mathbb{N}$.

  Toutefois, l'ensemble des entiers relatifs n'a pas une structure de groupe pour la multiplication : 5 n'a pas de symétrique pour la multiplication (ici symétrique pour la multiplication = inverse), $\dfrac{1}{5}$ n'est pas un élément de $\mathbb{Z}$. Il a donc été nécessaire de construire un nouvel ensemble dans lequel tous les nombres ont un inverse : $\mathbb{Q}$.

- Les autres ensembles se sont créés sur cette logique : puisque l'ensemble le plus vaste connu à l'heure actuelle ne permet pas de faire telle ou telle opération alors on en invente un nouveau. Quitte à ce que cela défie la logique et se fasse de façon tout à fait artificielle : c'est le cas pour la construction de l'ensemble $\mathbb{R}$ à partir de $\mathbb{Q}$.

  On peut aussi citer l'ensemble des nombres complexes, noté $\mathbb{C}$, qui fut créer pour que tous les nombres négatifs possèdent un carré.

Un axiome est une vérité indémontrable, un postulat de départ évident qui ne se démontre pas mais doit se comprendre parfaitement.

- Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
- Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.
- Toute suite d'entiers naturels strictement décroissante est finie.
- Toute suite d'entiers naturels strictement décroissante est finie.

Remarque 2.1 :

Cet axiome est faux dans $\mathbb{Z}$: Prenons la suite (u_n) définie par $u_n = -n$. Cette suite est à valeur dans $\mathbb{Z}$ et est strictement décroissante. Cependant elle n'est pas finie.

I. Multiples et diviseurs dans $\mathbb{Z}$

Définition 2.2 : Multiple et Diviseur

On considère deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.

On dit que b divise a si et seulement si il existe ....

....

Pour b divise a, on note ....

On peut aussi formuler de la manière suivante :

- ....
- ....
- ....

Exemple 2.3 :

- $45 = 9 \times 5$ ....
  ....
  ....
  ....
- Les diviseurs dans $\mathbb{Z}$ de 6 sont : ....
  ....
  ....
  ....

Remarque 2.4 :

- ....
  ....
- ....
  ....

Exemple 2.5 :

Etant donné un nombre $n \in \mathbb{N}$, écrire une fonction Python appelée ListeDiviseurs, qui renvoie une liste contenant l'ensemble des diviseurs dans $\mathbb{N}$.

....

....

....

....

....

....

....

....

Complément(s) :

Exercice Résolu 1 p. 177 « Caractériser la divisibilité »

Complément(s) :

Exercice Résolu 2 p. 117 « Déterminer et utiliser la liste des diviseurs »

✎ ***Exercice(s) :***

Exercices 1 et 2 p. 126

Complément(s) :

Vidéo « Utiliser la définition de la divisibilité ».

Propriété 2.6 :

On considère deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.

....

....

Démonstration 2.7 :

On considère deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.

....

....

....

....

....

....

....

....

Propriété 2.8 : ***Transitivité de la division***

On considère trois entiers $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$.

....

....

Démonstration 2.9 :

On considère trois entiers $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$.

....

....

....

....

....

....

Exemple 2.10 :

60 est divisible par 10 et 10 est divisible par 5 donc 60 est divisible par 5.

✎ ***Exercice(s) :***

Exercices 8 et 17 p. 126

Propriété 2.11 : — Stabilité par combinaison linéaire de la division

On considère trois entiers $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$.

....

....

....

....

Démonstration 2.12 :

On considère trois entiers $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$.

....

....

....

....

....

....

Remarque 2.13 :

En particulier, la propriété précédente nous donne le résultat suivant :

Si a divise b et si a divise c alors a divise $b+c$ et a divise $b-c$.

Exemple 2.14 :

On considère un entier naturel k et on pose $a = 9k+2$ et $b = 12k+1$.

Quels peuvent être les diviseurs positifs communs à a et b ?

....

....

....

....

....

....

Complément(s) :

Exercice Résolu 4 p. 117 « Utiliser une combinaison linéaire »

Complément(s) :

Vidéo « Utiliser la définition de la divisibilité ».

✎ ***Exercice(s) :***

Exercice 9 p. 126

II. Division euclidienne

Activité 2.15 :

Toute personne en France métropolitaine et dans les départements d'outre-mer (DOM) est inscrite au répertoire national d'identification des personnes physiques (RNIPP). L'inscription à ce répertoire entraine l'attribution du numéro d'inscription au répertoire (NIR) par l'INSEE (Institut National des Statistiques et des Etudes Economiques). Ce numéro est utilisé notamment par les organismes d'assurance maladie pour la délivrance des cartes vitales.

Le NIR est communément appelé « numéro de sécurité sociale » ou « numéro INSEE ».

Ce numéro est constitué de 15 chiffres. En lisant de gauche à droite, on a :

- Le premier chiffre est 1 s'il s'agit d'un homme et 2 s'il s'agit d'une femme ;
- Les deux chiffres suivants désignent les deux derniers chiffres de l'année de naissance ;
- Les deux chiffres suivants désignent le mois de naissance ;
- Les cinq chiffres suivants désignent le lieu de naissance : en général, les deux chiffres du numéro de département de naissance suivis des trois chiffres répertoriant la commune de naissance ;
- Les trois chiffres suivants désignent le numéro d'inscription sur le registre d'état civil ;
- Les deux derniers chiffres résultent d'un calcul.

Objectif : savoir comment détecter une erreur dans le numéro de sécurité sociale.

1. Pour chacun des numéros de sécurité sociale, effectuer les opérations suivantes sur tableur :
   - A l'aide de la fonction MOD, calculer le reste r de la division euclidienne des 13 premiers chiffres des numéros de sécurité sociale précédents par 97
   - Calculer $97 - r$.
   - Que constatez-vous ?

   (a) 2 77 08 44 109 048 91 (b) 1 16 10 17 192 162 26 (c) 2 26 04 29 189 222 66

Activité 2.15 (suite) :

1. Quel sera le numéro de sécurité sociale d'un garçon né le 26 juillet 2011 dans le département de la Gironde (33 représente) dans la commune de Libourne (243) enregistré au registre des naissances de l'état civil sous le numéro 136 ?

   ....

2. Parmi les numéros de sécurité sociale suivants, déterminer ceux qui ne sont pas corrects :

   - 2 85 07 86 183 084 15
   - 2 85 07 86 183 048 15
   - 2 85 07 86 183 049 15

Les deux derniers chiffres du numéro de sécurité sociale constituent la clé de contrôle du numéro. C'est grâce à cette clé que l'on peut détecter certaines erreurs.

Définition 2.16 : ***Division euclidienne dans $\mathbb{N}$***

On considère deux entiers $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$.

....

....

....

....

....

....

Exemple 2.17 :

Effectuer la division euclidienne de 343 par 12.

....

....

....

....

Complément(s) :

Exercice Résolu 1 p. 119 « Ecrire une division euclidienne »

Complément(s) :

Vidéo « Déterminer le quotient et reste d'une division euclidienne ».

Définition 2.18 : ***Division euclidienne dans $\mathbb{Z}$***

On considère deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.

....

....

....

....

....

Exemple 2.19 :

Effectuer le division euclidienne de 431 par -17 puis de -121 par -9.

....

....

....

....

....

Complément(s) :

Vidéo « Déterminer le quotient et reste d'une division euclidienne (en fonction de n) ».

Complément(s) :

Vidéo « Démontrer une divisibilité par disjonction de cas ».

✎ ***Exercice(s) :***

Exercices 19, 21 et 30 page 126

III. Congruence

Définition 2.20 : ***Congruence***

On considère n un entier naturel ($n \geqslant 2$) et deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.

On dit que deux entiers a et b sont congrus modulo n si et seulement si ....

....

On note alors :

....

On le lit : ....

Exemple 2.21 :

Montrer que 57 est congru à 15 modulo 7.

. . . .

. . . .

. . . .

. . . .

. . . .

✎ ***Exercice(s) :***

Exercices 33 et 34 p. 127

Propriété 2.22 : — Congruence = Relation d'équivalence

La congruence est une relation d'équivalence :

- Elle est réflexive : . . . .
- Elle est symétrique : . . . .
- Elle est transitive : . . . .

Exemple 2.23 :

Montrer que $15 \equiv 1\ [7]$ et en déduire que $57 \equiv 1\ [7]$.

. . . .

. . . .

. . . .

. . . .

. . . .

. . . .

Théorème 2.24 :

On considère un entier naturel n ($n \geqslant 2$) ainsi que deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.

. . . .

. . . .

Théorème 2.25 : — Sommes, produits et puissances de congruences

On considère $n \in \mathbb{N}$ ($n \geqslant 2$) et a, b, c et d des éléments de $\mathbb{Z}$ vérifiant :

$$a \equiv b\ [n] \qquad \text{et} \qquad c \equiv d\ [n]$$

Alors on a les propriétés suivantes :

- ....
- ....
- Pour tout $k \in \mathbb{N}$, on a :

  ....

Exercice(s) :

Exercice 36 p. 127

Complément(s) :

Exercice Résolu 3 p. 121 « Déterminer le reste d'une division euclidienne avec les congruences »

Exemple 2.26 :

Déterminer les restes dans la division par 7 des nombres suivants : 50^{100}, 100, 100^3 et $50^{100} + 100^{100}$.

....

....

....

....

....

....

....

....

....

....

....

....

....

....

Complément(s) :

Exercice Résolu 2 p. 121 « Montrer une divisibilité à l'aide les congruences »

Exemple 2.27 :

Montrer que pour tout $n \in \mathbb{N}$, $3^{n+3} - 4^{4n+2}$ est divisible par 11.

....

....

....

....

....

....

....

....

....

....

....

Complément(s) :

Exercice Résolu 1 p. 121 « Résoudre des équations avec les congruences »

✎ ***Exercice(s) :***

Exercices 38 et 40 p. 127

IV. Applications

1. Changements de bases

Notre système de numérotation est un système décimal de position. Il est constitué de 10 chiffres dont le position indique le nombre d'unités de la puissance de 10 correspondante.

Exemple 2.28 :

$3406 = 3 \times 10^3 + 4 \times 10^2 + 0 \times 10^1 + 6 \times 10^0$

De manière générale, si on considère un entier naturel A écrit en base 10 avec $n+1$ chiffres et si l'on note a_0 le chiffre des unités, a_1 le chiffre des dizaines, a_3 le chiffres des centaines, etc, alors :

$$A = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \ldots + a_1 \times 10^1 + a_0 \times 10^0$$

où chaque a_i désigne un nombre entier compris entre 0 et 9.

Définition 2.29 : **Ecriture décimale**

Dans un système de position en base b, on note un nombre entier par $A = \overline{a_n a_{n-1} \dots a_1 a_0}^b$. Ce nombre A sécrit dans ce système décimal par :

$$A = \overline{a_n a_{n-1} \dots a_1 a_0}^b = a_n \times b^n + a_{n-1} \times b^{n-1} + \dots + a_1 \times b^1 + a_0 \times b^0$$

où chaque a_i sont des entiers inférieurs ou égaux à $b - 1$.

Exemple 2.30 :

$34 = \overline{1021}^3 = 1 \times 3^3 + 0 \times 3^2 + 2 \times 3^1 + 1 \times 3^0$

Exemple 2.31 :

Convertir en base 10 les nombres suivants :

1. $\overline{110111}^2$ ....
   ....
2. $\overline{231}^5$ ....
   ....
3. $\overline{13051}^8$ ....
   ....
4. $\overline{402}^7$ ....
   ....

Remarque 2.32 :

Dans le système décimal (en base 10) les chiffres utilisés dans l'écriture des nombres sont : 0 ; 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 6 ; 7 ; 8 ; 9.

Dans le système binaire (en base 2) les chiffres sont : 0 et 1.

Si on doit écrire un nombre dans une base plus grande que 10, on devra compléter par d'autres symboles (généralement des lettres). Ainsi si on doit écrire en base 12 (duodécimal), on utilisera les chiffres de 0 à 9 et les lettres A et B pour 10 et 11.

Exemple 2.33 :

Convertir en base 10 les nombres suivants :

1. $\overline{A1650}^{12}$ ....
   ....
2. $\overline{A150}^{16}$ ....
   ....
3. $\overline{1C0D}^{16}$ ....
   ....

Méthodologie 2.34 : — ***Passage de la base*** 10 ***à la base*** b

Pour déterminer l'écriture d'un nombre dans notre système de numérotation vers un système de numérotation en base b, on effectue des divisions successives de ce nombre par b.

On obtient le nombre en base b en effectuant les divisions successives des restes par b jusqu'à obtenir un quotient nul. Le chiffre obtenu se lit en remontant les restes.

Exemple 2.35 :

Donner l'écriture des nombres suivants :

1. 2 278 en base 7

   ....
   ....
   ....
   ....
   ....
   ....
   ....
   ....
   ....
   ....
   ....
   ....
   ....

Exemple 2.35(suite) :

2. 2 278 en base 12

....

....

....

....

....

....

....

....

....

....

....

....

....

3. 149 en base 2

....

....

....

....

....

....

....

....

....

....

....

....

....

2. Critères de divisibilité

On considère un nombre $n = \overline{a_p a_{p-1} ... a_1 a_0}^{10}$. L'objectif de cette partie est de retrouver les critères de divisibilités par 2, 3, 5, 9 et 11.

Propriété 2.36 : ***Divisibilité par 2***

On considère un entier $n \in \mathbb{N}$.

n est divisible par 2 si et seulement si son chiffre des unités est divisible par 2 (c'est-à-dire si son chiffre des unités est 0, 2, 4, 6 ou 8).

Démonstration 2.37 :

Démontrer le résultat en décomposant n selon les puissances de 10.

....

....

....

....

....

....

Propriété 2.38 : ***Divisibilité par 3***

On considère un entier $n \in \mathbb{N}$.

n est divisible par 3 si et seulement si ....

....

Démonstration 2.39 :

- Montrer que pour tout $k \in \mathbb{N}$, on a $10^k \equiv 1 \ [3]$.

  ....

  ....

  ....

  ....

Démonstration 2.39 (suite) :

- En déduire le critère de divisibilité par 3.

....

....

....

....

....

....

....

....

....

Propriété 2.40 : Divisibilité par 5

On considère un entier $n \in \mathbb{N}$.

n est divisible par 5 si et seulement si ....

....

Démonstration 2.41 :

- Montrer que pour tout $k \in \mathbb{N}^*$, $10^k \equiv 0\ [5]$.

....

....

....

....

- En déduire le critère de divisibilité par 5.

....

....

....

....

....

....

....

....

....

Propriété 2.42 : — Divisibilité par 9

On considère un entier $n \in \mathbb{N}$.

n est divisible par 9 si et seulement si ....

....

Démonstration 2.43 :

- Montrer que pour tout $k \in \mathbb{N}$, on a $10^k \equiv 1\ [9]$.

  ....

  ....

  ....

- En déduire le critère de divisibilité par 9.

  ....

  ....

  ....

  ....

  ....

  ....

  ....

  ....

  ....

Propriété 2.44 : — Divisibilité par 11

On considère un entier $n \in \mathbb{N}$.

n est divisible par 11 si et seulement si ....

....

Démonstration 2.45 :

- Montrer que pour tout $k \in \mathbb{N}$, on a $10^k \equiv (-1)^k\ [10]$.

  ....

  ....

  ....

  ....

  ....

  ....

Démonstration 2.45 (suite) :

- Ecrire le résultat précédent selon la parité de k.

  ....

  ....

- En déduire le critère de divisibilité par 11.

  ....

  ....

  ....

  ....

  ....

  ....

  ....

  ....

  ....

3. Calendriers

✎ ***Exercice(s) :***

L'objectif de ce problème est de déterminer quel jour de la semaine fut le 14 juillet 1789.

1. Sans tenir compte des années bissextiles, combien de jours séparent le 14 juillet 2014 du 14 juillet 1789 ?
2. Sachant que les années bissextiles sont les années divisibles par 4, calculer le nombre d'années bissextiles.
3. Sauf que les années divisibles par 100 ne sont pas bissextiles, alors réajuster le nombre d'années bissextiles entre 1789 et 2014.
4. Sauf que les années divisibles par 400 sont bissextiles, alors réajuster le nombre d'années bissextiles entre 1789 et 2014.
5. Combien de jours séparent alors le 14 juillet 2014 du 14 juillet 1789 ?
6. Calculer le reste de la division euclidienne de ce nombre par 7.
7. Sachant que le 14 juillet 2014 est un lundi, en déduire quel jour était le 14 juillet 1789.