Chapitre 1

Divisibilité

I Exercices

1.1 Divisibilité

Exercice 1.1

Déterminer tous les rectangles à côtés entiers d'aire 24 cm^2.

Exercice 1.2

Déterminer les points à coordonnées entières qui sont sur la droite d'équation $y = 13x$ dont l'ordonnée est comprise entre 200 et 230.

Exercice 1.3

1. Peut-on écrire la liste de tous les multiples de 12 ? Si la réponse est oui, écrire cette liste.
2. Peut-on écrire la liste de tous les diviseurs de 12 ? Si la réponse est oui, écrire cette liste.

Exercice 1.4

Pour chacune des affirmations ci-dessous, indiquer si elle est vraie ou fausse, en justifiant.

1. Tous les nombres entiers sont multiples de zéro.
2. Zéro est multiple de tous les nombres entiers.
3. Tous les nombres entiers sont multiples de 1.
4. 1 est multiple de tous les nombres entiers.

Exercice 1.5

Est-ce que pour tout nombre entier n, le nombre $n + 4$ est multiple de 2 ?

Si la réponse est oui, justifier pourquoi.

Si la réponse est non, pour quelles valeurs de n le nombre $n + 4$ est multiple de 2 ? Justifier.

Exercice 1.6

Pour un entier x, le nombre $9x^2 - 25$ est-il un multiple $3x - 5$?

Exercice 1.7

Lorsque n est un nombre entier, le nombre $3n + 12$ est-il multiple de 3 ? Justifier.

Exercice 1.8

1. Dans le repère de la figure 1.1 tracer la droite (d) d'équation cartésienne $6x - 2y = 5$.
2. La droite (d) a-t-elle des points à coordonnées entières ?

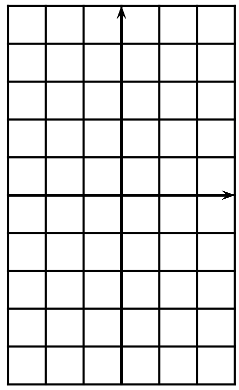

Fig. 1.1

Exercice 1.9

Déterminer les entiers n tels que $2n - 3$ divise 4.

Exercice 1.10

Déterminer les entiers naturels x et y tels que $x^2 - y^2 = 49$

Exercice 1.11

La somme de trois entiers consécutifs est-elle divisible par 3 ? Justifier.

Exercice 1.12

Démontrer que si n est multiple de 3, alors $n(n^2 + 18)$ est multiple de 27.

Exercice 1.13

Déterminer tous les triangles rectangles à côtés entiers tels qu'un côté de l'angle droit mesure 6 cm.

1.2 Propriétés de la divisibilité

Exercice 1.14

Un nombre entier a divise deux nombres entiers b et c, ce qui signifie que b et c sont multiples de a.

1. Le nombre a divise-t-il la somme $b + c$? Justifier.
2. Le nombre a divise-t-il la différence $b - c$? Justifier.
3. Pour deux autres entiers u et v, le nombre a divise-t-il la combinaison linéaire $bu+cv$? Justifier.

Exercice 1.15

Déterminer les entiers n tels que $n + 3$ divise $n + 5$. Indication : $n + 3$ divise $n + 3$.

Exercice 1.16

Déterminer les entiers n tels que $3n - 1$ divise $n - 2$.

1.3 Division euclidienne

Exercice 1.17 (Un code et sa clef de contrôle)

Un site Internet a prévu un système de numéro d'inscription à huit chiffres et une clef de contrôle à deux chiffres. On appelle a le nombre constitué par les huit chiffres. La clef de contrôle est le reste de la division euclidienne du nombre a par 97.

Prenons un exemple avec $a = 12\,345\,678$. La division euclidienne de a par 97 s'écrit :

$a = 12\,345\,678 = 97 \times 127\,275 + 3$.

Le reste de cette division est donc 3, ce qui donne 03 comme clef de contrôle. L'utilisateur saisit donc `12 345 678|03` et le site vérifie si `03` est bien la clef de contrôle de `12 345 678`.

1. Calculer la clef de contrôle du numéro `10 200 300`.
2. Un utilisateur saisit `10 200 345|17`
   a) Vérifier que ce numéro d'inscription est faux.
   b) L'utilisateur s'est trompé sur le dernier chiffre du numéro d'inscription c'est à dire le chiffre 5. Rectifier son erreur.

Exercice 1.18 (Code-barre et ISBN)

Les codes-barres figurent sur de nombreux articles vendus dans le commerce. Le code-barre d'un article est son numéro d'identification, c'est un numéro à 13 chiffres et son dernier chiffre est une clef de contrôle. Depuis 2007, le numéro ISBN, qui est réservé aux livres, utilise le même type de numérotation.
Le code-barre `9788073400972` est représenté sur la figure 1.2.

9 788073 400972

Fig. 1.2

On détermine sa clef de contrôle comme cela est indiqué ci-dessous.

- Dans les douze premiers chiffres,
  ▷ on calcule la somme des chiffres de rang impair : $S_1 = 9 + 8 + 0 + 3 + 0 + 9 = 29$;
  ▷ on calcule la somme des chiffres de rang pair : $S_2 = 7 + 8 + 7 + 4 + 0 + 7 = 33$.
- On calcule : $S = S_1 + 3S_2 = 29 + 3 \times 33 = 128$.
- On détermine le reste r de la division euclidienne de S par 10 : $r = 8$, puisque $128 = 10 \times 12 + 8$.
- La clef de contrôle est $10 - r = 10 - 8 = 2$.

Voici un code barre sans sa clef de contrôle c'est à dire avec ses douze premiers chiffres seulement : `978209172673`. Déterminer sa clef de contrôle.

Si l'on veut en savoir plus sur le code-barre et sur l'ISBN, voir le problème n° 8 pages 13, 14, 15 du manuel Hyperbole TS spécialité math.

Exercice 1.19

Effectuer la division euclidienne de a par b dans chacun des cas suivants. Écrire sa réponse sous la forme $a = bq + r$.

1. Sans calculatrice :

   a) $a = 26 \quad b = 3$ **b)** $a = 534 \quad b = 10$ **c)** $a = 837\,329 \quad b = 100$

2. Avec calculatrice :

   a) $a = 453 \quad b = 17$ **b)** $a = 2\,358 \quad b = 43$ **c)** $a = 54\,200 \quad b = 147$

Exercice 1.20

Comment obtient-on sans calcul le reste de la division d'un nombre entier par 10 ? par 100 ? par 1 000. Donner des exemples.

Exercice 1.21

1. a) Vérifier l'égalité $2\,882 = 23 \times 124 + 30$
   b) Ce calcul ne donne pas le quotient et le reste de la division euclidienne de $2\,882$ par 23. Pourquoi ?

2. Pour chacune des égalités suivantes, indiquer si l'égalité permet de donner le quotient et le reste de la division de a par b. Si la réponse est non, donner l'égalité correcte.

   a) $a = 267 \quad b = 18 \qquad 267 = 18 \times 12 + 51$ **b)** $a = 3\,527 \quad b = 73 \qquad 3\,527 = 73 \times 48 + 23$
   c) $a = 309 \quad b = 7 \qquad 309 = 7 \times 43 + 8$

Exercice 1.22

1. Donner toutes les divisions euclidiennes possibles de diviseur 4 et de quotient 12.
2. Donner toutes les divisions euclidiennes possibles de dividende 83 et de quotient 5.

Exercice 1.23

Une année non bissextile commence un lundi. Calculer le jour de la semaine correspondant au

1. 25 janvier **2.** 20 avril

Après avoir abordé la divisibilité, puis la division euclidienne, l'exercice ci-dessous permet de faire le lien entre divisibilité et la division euclidienne.

Exercice 1.24

1. **a)** Effectuer la division euclidienne de $9\,953$ par 37.
   b) $9\,953$ est-il divisible par 37 ?
2. Mêmes questions **a)** et **b)** pour $10\,511$ par rapport à 53.
3. Pour un nombre entier a et un nombre entier b non nul, lorsque a est divisible par b, que peut-on dire de la divison euclidienne de a par b ?

1.4 Congruences

Dans tous les exercices sur les congruences modulo n, n désigne un entier naturel supérieur ou égal à 2.

Exercice 1.25

Lire dans le cours la définition 1.4 (congruence modulo n), puis répondre aux questions ci-dessous.

1. Indiquer chaque fois si c'est vrai ou faux. Justifier.

   a) $53 \equiv 13\ [10]$ **b)** $35 \equiv 21\ [5]$ **c)** $88 \equiv 70\ [9]$ **d)** $17 \equiv -1\ [6]$ **e)** $14 \equiv -2\ [3]$

2. Compléter ci-dessous.

   a) $11 \equiv 5\ [\ldots]$ **b)** $26 \equiv 12\ [\ldots]$ **c)** $87 \equiv 62\ [\ldots]$ **d)** $7 \equiv -3\ [\ldots]$

3. Compléter ci-dessous.

   a) $17 \equiv \ldots\ [2]$ **b)** $43 \equiv \ldots\ [5]$ **c)** $\ldots \equiv 30\ [7]$ **d)** $\ldots \equiv -4\ [10]$

4. L'affirmation ci-dessous est-elle vraie ou fausse ? Justifier.
   $a \equiv 0\ [n] \iff a$ est multiple de n

Exercice 1.26 (Conséquence de la définition pour la division euclidienne)

1. **a)** Écrire la division euclidienne de 38 par 5 et déterminer le reste.
   b) 38 est-il congru à ce reste modulo 5 ?

2. Pour un entier a, si r est le reste de la division euclidienne de a par n le nombre a est-il congru à r modulo n ?

3. **a)** Justifier que $38 \equiv 8\ [5]$.

b) Le reste de la division euclidienne de 38 par 5 est-il égal à 8 ?

4. Si $a \equiv r\ [n]$, le nombre r est-il le reste de la division euclidienne de a par n ? Si la réponse est non, quelle condition faut-il ajouter pour que ce soit toujours vrai ?

Exercice 1.27

Dans chacun des cas suivants, a et n sont des entiers naturels. Calculer chaque fois le nombre entier naturel b tel que $a \equiv b\ [n]$ et $0 \leqslant b < n$.

1. Sans calculatrice :

a) $a = 44 \quad n = 6$ **b)** $a = 763 \quad n = 2$ **c)** $a = 829 \quad n = 10$ **d)** $a = 73\,956 \quad n = 100$

2. Avec calculatrice :

a) $a = 328 \quad n = 17$ **b)** $a = 4\,657 \quad n = 38$ **c)** $a = 1\,327 \quad n = 148$

Exercice 1.28 (Congruence et division euclidienne – Une propriété importante)

1. 23 et 17 ont-ils le même reste dans la division euclidienne par 3 ?

2. Vérifier si 23 est congru à 17 modulo 3.

La généralisation de cette propriété est la propriété 1.9 du cours.

Exercice 1.29 (Congruence et opérations)

1. Justifier que $61 \equiv 19\ [7]$ et $36 \equiv 22\ [7]$.

2. Vérifier que :

(1) $61 + 36 \equiv 19 + 22\ [7]$ **(2)** $61 - 36 \equiv 19 - 22\ [7]$

(3) $61 \times 36 \equiv 19 \times 22\ [7]$ **(4)** $61^3 \equiv 19^3\ [7]$

Les généralisations de ces propriétés sont regroupées dans la propriété 1.10 du cours. C'est ce qui va nous permettre de simplifier considérablement les calculs.

Étudier l'exemple du paragraphe 1.3.b du cours, puis traiter l'exercice ci-dessous.

Exercice 1.30 (Reste de la division d'un grand nombre)

Déterminer le reste de la division de $33\,000\,000\,000\,000$ par 7.

Exercice 1.31 (Clef de contrôle d'un numéro de RIB)

Le numéro d'un compte bancaire est nommé relevé d'identité bancaire (RIB).

En voici un exemple sans la clef de contrôle :

Code banque	Code guichet	Numéro de compte	Clé RIB
12802	00750	20741300623	

On appelle a le nombre $12\,802\,007\,502\,074\,130\,062\,300$

La clef de contrôle sert à vérifier s'il n'y a pas eu d'erreur de saisie sur les 21 premiers chiffres et elle est définie de la manière suivante : si r est le reste de la division euclidienne de a par 97, la clef est $97 - r$.

Calculer cette clef de contrôle.

Indication : pour calculer le reste de la division euclidienne de a par 97, on pourra décomposer par exemple ce nombre ainsi : $a = 12\,802\,007\,502 \times 10^{12} + 74\,130\,062\,300$ et on a tout intérêt à effectuer les divisions euclidiennes par 97 à l'aide d'un programme.

Exercice 1.32 (Clef de contrôle d'un numéro d'INSEE)

En France, l'INSEE [1] attribue à tout individu en France un numéro d'INSEE [2] constitué de 13 chiffres et de 2 chiffres supplémentaires qui sont une clef de contrôle.

Le numéro d'INSEE d'une personne sans la clef de contrôle est 2 87 04 06 164 068.

La clef de contrôle est définie de la manière suivante : si r est le reste de la division euclidienne de $2\,870\,406\,164\,068$ par 97, la clef est $97 - r$.

Calculer cette clef de contrôle.

1.5 Numération

La numération est la façon d'écrire les nombres. Il y a eu des numérations comme les numérations maya, égyptienne, romaine, etc. Notre numération décimale vient des indiens et des arabes.

Lire l'exemple et les explications ci-dessous avant de commencer les exercices.

Exemple : le nombre 493 est égal à $4 \times 100 + 9 \times 10 + 3$.

Plus généralement un nombre entier naturel à trois chiffres qui s'écrit $\overline{abc}$ est égal à $a \times 100 + b \times 10 + c$ où a, b, c, sont des nombres entiers entre 0 et 9.

Exercice 1.33 (Critère de divisibilité par deux)

Le chiffre des unités d'un nombre entier naturel est 6, autrement dit ce nombre s'écrit $\overline{ab6}$.

Démontrer que ce nombre est multiple de 2.

C'est ainsi qu'on démontre le critère de divisibilité par deux.

Exercice 1.34 (Critère de divisibilité par cinq)

Démontrer le critère de divisibilité par cinq pour un nombre entier naturel à trois chiffres. Il y aura deux cas à étudier.

Exercice 1.35 (Critère de divisibilité par trois)

On considère un nombre entier naturel à trois chiffre $\overline{abc}$.

1. Démontrer que $\overline{abc} \equiv a + b + c\ [3]$.
2. Démontrer le critère de divisibilité par trois pour un nombre entier naturel à trois chiffres.

Exercice 1.36

Pour un nombre entier naturel n, quels sont les chiffres des unités possibles de $n^2 + n$? Justifier.

1.6 Exercices divers

Exercice 1.37

Déterminer le reste de la division euclidienne de 5^{2018} par 7.

Indication : étudier d'abord les congruences modulo 7 de 5, 5^2, 5^3, etc.

1. L'INSEE est l'Institut National de la Statistique et des Études Économiques.
2. Détails du numéro d'INSEE dans le manuel Hyperbole 1re S, problème 7 page 13.

Exercice 1.38

Quels sont les entiers n tels que $n^4 - 1$ est multiple de 5 ?

Indication : étudier d'abord les congruences modulo 5 de n, n^2, n^4.

Exercice 1.39

1. Donner l'expression numérique qui permet de calculer $1 + 7 + 7^2 + \cdots + 7^{2017}$.

2. Le nombre $7^{2018} - 1$ est-il divisible par 6 ? Justifier.

Exercice 1.40

1. Résoudre les équations :

a) $2x \equiv 3\ [5]$ **b)** $5x \equiv 2\ [3]$ **c)** $7x \equiv 25\ [53]$

2. Résoudre les équations :

a) $x^2 \equiv 4\ [6]$ **b)** $x^2 \equiv 3\ [6]$ **c)** $x^2 \equiv 2\ [6]$

d) $x^2 \equiv 2\ [7]$ **e)** $x^2 \equiv 1\ [33]$ **f)** $x(x + 17) \equiv 33\ [55]$

1.7 Pour réviser

Chapitre du livre n° 1 – Divisibilité dans $\mathbb{Z}$

Les exercices résolus

- ex 1 p 9 : divisibilité entre expressions en fonctions de n.
- ex 7 p 11 : division euclidienne entre expressions en fonctions de n.
- ex 15 p 17 : congruences, démontrer que $n(n^2 + 5)$ est divisible par 3.
- ex 16 p 17 : reste de la division euclidienne par de 23^{41} par 7.

Rubrique *Pour s'exercer*, corrigés page 156

- ex 3 p 9 : divisibilité entre expressions en fonctions de n.
- ex 5 p 9 : équation en nombres entiers
- ex 12 p 11 : division euclidienne entre expressions en fonctions de n.
- ex 18 p 17 : congruence
- ex 22 p 17 : reste de la division euclidienne par de 12^{1527} par 5.

Rubrique *Objectif bac*, corrigés page 158

- ex 101 p 28 (QCM) : questions 1 à 5
- ex 103 p 28 : questions 1 et 2

II Cours

1.1 Divisibilité

1.1.a Les nombres entiers

Ce chapitre, ainsi que les chapitres sur les théorèmes de Bézout et Gauss, et sur les nombres premiers porteront sur l'arithmétique, c'est à dire sur des calculs avec des nombres entiers.

Ce premier paragraphe est donc une mise au point sur les nombres entiers.

Définition 1.1 (Nombres entiers)

- Un nombre entier est un nombre entier relatif c'est à dire un nombre entier négatif, nul ou positif.
- Un nombre entier naturel est un nombre entier positif ou nul.
- L'ensemble des nombres entiers (relatifs) est noté $\mathbb{Z}$.
- L'ensemble des nombres entiers naturels est noté $\mathbb{N}$.

Propriété 1.1 (Opérations entres nombres entiers)

Pour deux nombres entiers a et b,

- La somme $a+b$, la différence $a-b$, le produit ab sont des nombres entiers.
- le quotient $\dfrac{a}{b}$ $(b \neq 0)$ de deux nombres entiers n'est pas toujours un nombre entier.

Remarque

La conséquence fondamentale de la propriété 1.1 est qu'en arithmétique, on utilisera exclusivement l'addition, la soustraction et la multiplication.

1.1.b Définitions

Définition 1.2 (Divisibilité)

Dire qu'un nombre entier a est divisible par un nombre entier b non nul signifie qu'il existe un nombre entier k tel que $a = b \times k$.

Définition 1.3 (Divisible, multiple, diviseur, divise)

Pour deux nombres entiers a et b, les expressions suivantes sont équivalentes :

- a est divisible par b ;
- a est multiple de b ;
- b est un diviseur de a.
- b divise a.

Exemple

14 est divisible par 2, puisque : $14 = 2 \times 7$ et on dit aussi que 14 est multiple de 2 ou que 2 est un diviseur de 14 ou encore que 2 divise 14.

1.1.c Propriétés de la divisibilité

Propriété 1.2

Pour trois nombres entiers a, b, c, si a divise b et b divise c alors a divise c.

Démonstration

Pour trois nombres entiers a, b, c, si a divise b et b divise c, cela signifie qu'il existe k et k' tels que $b = ka$ et $c = k'b$. Par conséquent $c = k'ka$ autrement dit a divise c.

Remarque

La propriété précédente est très simple à démontrer, mais elle est importante et servira très souvent.

Ce type de propriété est important en mathématiques. on appelle cela la transitivité : si a est en relation avec b et b en relation avec c, alors a est en relation avec c.

On retrouve la transitivité pour les relations d'égalité, d'infériorité, de parallélisme, d'inclusion.

Propriété 1.3

Pour trois nombres entiers a, b, c, si a divise b et c, alors a divise $b + c$ et $b - c$.
Autrement dit, pour trois nombres entiers,
si un nombre divise deux autres nombres, alors il divise leur somme et leur différence.

Démonstration

Pour trois nombres entiers a, b, c, dire que a divise b et c signifie qu'il existe des entiers k et k' tels que $b = ak$ et $c = ak'$.

Par conséquent : $b + c = ak + ak' = a(k + k')$ et $b - c = ak - ak' = a(k - k')$.

Donc : a divise $b + c$ et $b - c$.

Propriété 1.4

Pour trois nombres entiers a, b, c, si a divise b et c, alors, pour tous entiers u et v, a divise $bu + cv$.
Autrement dit, pour trois nombres entiers,
si un nombre divise deux autres nombres, alors il divise toute combinaison linéaire à coefficients entiers de ces deux nombres.

Démonstration

a divise b et c donc il existe des entiers k et k' tels que $b = ak$ et $c = ak'$.

Par conséquent : $bu + cv = aku + ak'v = a(ku + k'v)$ donc a divise $bu + cv$.

1.2 La division euclidienne

1.2.a Propriété et exemples

Propriété 1.5 (Division euclidienne)

Pour un nombre entier a et un nombre entier naturel non nul b, il existe un seul couple de nombres entiers (q, r) tel que : $a = bq + r$ et $0 \leqslant r < b$.

Remarques

- On peut traduire la propriété 1.5 par :
  dividende = diviseur × quotient + reste et reste < diviseur
- La propriété 1.5 évoque la division euclidienne d'un entier a (relatif) par un entier naturel b (positif), autrement dit un dividende positif ou négatif par un diviseur strictement positif. On peut en fait avoir un diviseur b non nul positif ou négatif et on écrit alors :
  $a = bq + r$ et $0 \leqslant r < |b|$.

Un exemple avec des petits nombres

Une division euclidienne pour des petits nombres est effectuée à l'aide des tables de multiplication, par exemple la division euclidienne de 27 par 4 : $27 = 4 \times 6 + 3 \; ; \; 3 < 4$

Un exemple avec des plus grands nombres

Effectuons par exemple la division euclidienne de 13 473 par 37.

Calculons d'abord le quotient décimal à la calculatrice : $\dfrac{13\,473}{37} \approx 364,1$

Le quotient euclidien de la division euclidienne de 13 473 par 37 est donc la partie entière du résultat précédent, soit 364.

Calculons maintenant le reste : $13\,473 - 37 \times 364 = 5$

On a finalement : $13\,473 = 37 \times 364 + 5 \; ; \; 5 < 37$

1.2.b Utilisation des calculatrices

Reprenons l'exemple précédent : la division euclidienne de 13 473 par 37.

Division euclidienne avec les calculatrices TI

- **Quotient** Le quotient euclidien, est la partie entière de $\dfrac{13\,473}{37}$, donc :
  - on utilise les touches : $\boxed{\text{math}}$ $\boxed{\rightarrow}$ $\boxed{3}$
  - on complète ainsi : `ent(13473/37)`
  - on appuie sur $\boxed{\text{entrer}}$
  - Affichage : $\boxed{364}$
- **Reste avec la TI-82 Advanced ou la TI-83 Premium**
  - on utilise les touches : $\boxed{\text{math}}$ $\boxed{\rightarrow}$ $\boxed{0}$
  - on complète ainsi : `remainder(13473,37)` ou `reste(13473,37)`
  - on appuie sur $\boxed{\text{entrer}}$
  - Affichage : $\boxed{5}$
- **Calcul du reste sans la commande `reste` ou `remainder`**
  On calcule tout simplement : $13\,473 - 37 \times 364 = 5$.
  Si l'on veut calculer le reste en une seule suite de calculs :
  `13473-37*ent(13473/37)` Affichage : 5

Division euclidienne avec la CASIO

Appuyer sur la touche $\boxed{\text{MENU}}$ et choisir le module `RUN MAT`.

Appuyer sur les touches : $\boxed{\text{OPTN}}$ $\boxed{\text{F4}}$ (CALC) $\boxed{\text{F6}}$ ($\rightarrow$) $\boxed{\text{F6}}$ ($\rightarrow$)

- **Quotient**
  - saisir : `13473` $\boxed{\text{F1}}$ (`Int÷`) `37`
  - on voit : `13473 Int÷ 37`
  - appuyer sur $\boxed{\text{EXE}}$
  - Affichage : $\boxed{364}$
- **Reste**
  Même procédure que pour le quotient, en remplaçant $\boxed{\text{F1}}$ (`Int÷`) par $\boxed{\text{F2}}$ (`Rmdr÷`).

Division euclidienne avec la NUMWORKS

Dans l'application Calculs, on utilise la touche Toolbox : $\boxed{\text{paste"}}$

- **Quotient**
  - touche Toolbox
  - on choisit la rubrique `Arithmetique`
  - touche $\boxed{\rightarrow}$
  - descendre jusqu'à : `quo(p,q)`
  - appuyer sur $\boxed{\text{EXE}}$
  - on voit : `quo(,)`
  - compléter ainsi : `quo(13473,37)`
  - appuyer sur $\boxed{\text{EXE}}$
  - Affichage : $\boxed{364}$
- **Reste**

  Même procédure que pour le quotient, en remplaçant `quo(p,q)` par `rem(p,q)` et `quo(13473,37)` par `rem(13473,37)`.

1.2.c Utilisation des logiciels et de python3

	GeoGebra	LibreOffice	Xcas	wxMaxima	python3
Quotient de la division euclidienne de a par b	Quotient[a,b]	=QUOTIENT(a ;b)	iquo(a,b)	floor(a/b)	a//b
Reste de la division euclidienne de a par b	Reste[a,b]	=MOD(a ;b)	irem(a,b)	mod(a,b)	a%b
Division euclidienne de a par b	Division[a,b]		iquorem(a,b)	divide(a,b)	

1.2.d Division euclidienne et divisibilité

Propriété 1.6

Pour un nombre entier a et un nombre entier b non nul, dire que a est divisible par b signifie que le reste de la division euclidienne de a par b est zéro.

Démonstration

Dire qu'un nombre entier a est divisible par un nombre entier b non nul signifie qu'il existe un nombre entier k tel que $a = b \times k$, autrement dit $a = b \times k + 0$, ce qui signifie que le reste de la division euclidienne de a par b est zéro.

Remarque : cette propriété vient compléter la définition 1.3.

1.3 Congruence

Un des objectifs de ce chapitre est de pouvoir étudier différents système de codes qui utilisent la division euclidienne, comme dans l'exercice 1.17, avec des nombres ayant jusqu'à 23 chiffres, or les calculatrices, et mêmes les logiciels n'utilisent pas des nombres aussi longs.

Nous allons donc étudier une méthode de calculs, appelé *les congruences*, qui va permettre de réduire le nombre de chiffres à utiliser dans les calculs.

1.3.a Définition et propriétés

Définition 1.4 (Congruence modulo n)

Pour deux nombres entiers a et b, et pour un nombre entier naturel $n \geqslant 2$, dire que a est congru à b modulo n signifie que $a - b$ est multiple de n.
On écrit : $a \equiv b\ [n]$ ou $a \equiv b\ (n)$ ou $a \equiv b \pmod{n}$.

Exemple

$48 \equiv 13\ [5]$ parce que $48 - 13$ est multiple de 5, en effet : $48 - 13 = 35 = 5 \times 7$.

Propriété 1.7 (Conséquence de la définition pour la division euclidienne)

Pour un nombre entier a, un nombre entier naturel r et pour un nombre entier naturel $n \geqslant 2$,
- si r est le reste de la division euclidienne de a par n alors $a \equiv r\ [n]$;
- si $a \equiv r\ [n]$ et $0 \leqslant r < n$, alors r est le reste de la division euclidienne de a par n.

Exemple

$48 \equiv 3\ [5]$ parce que $48 - 3 = 45$ est multiple de 5, de plus $0 \leqslant 3 < 5$.

3 est bien le reste de la division euclidienne de 48 par 5 : $48 = 5 \times 9 + 3$

Démonstration

• Si r est le reste de la division euclidienne de a par n, alors $a = nq + r$, donc il existe un entier q tel que $a - r = nq$, de sorte que $a - r$ est multiple de n, par conséquent $a \equiv r\ [n]$.

• Si $a \equiv r\ [n]$ et $0 \leqslant r < n$, alors $a - r$ est multiple de n, donc il existe un entier k tel que $a - r = nk$ c'est à dire $a = nk + r$, et comme on sait que $0 \leqslant r < n$, on peut dire que r est le reste de la division euclidienne.

Propriété 1.8

Pour deux nombres entiers a et b, et pour un nombre entier naturel $n \geqslant 2$,
- $a \equiv a\ [n]$;
- si $a \equiv b\ [n]$, alors $b \equiv a\ [n]$;
- si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $a \equiv c\ [n]$.

Démonstration

- Pour tout entier a, $a - a = 0$, et comme 0 est multiple de n, on a bien : $a \equiv a\ [n]$.
- Pour tous entiers a et b, $a - b$ est multiple de n équivaut à $b - a$ est multiple de n.
- Si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $a - b$ et $b - c$ sont multiples de n, donc $a - b + b - c$ est multiple de n, donc $a - c$ est multiple de n, c'est à dire $a \equiv c\ [n]$.

Propriété 1.9 (Congruence et division euclidienne)

Pour deux nombres entiers a et b, et pour un nombre entier naturel $n \geqslant 2$,
$a \equiv b\ [n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Exemple

$35 \equiv 11\ [4]$ parce que $35 - 11 = 24 = 4 \times 6$

35 et 11 ont le même reste dans la division euclidienne par 4, en effet $35 = 4 \times 8 + 3$ et $11 = 4 \times 2 + 3$.

Remarque

Dans d'autres cours la définition de congruence est la propriété 1.9, et la définition 1.4 est considérée comme une propriété. C'est le cas par exemple dans le manuel Hyperbole de TS spécialité. Il faut de toute façon bien connaître les deux.

Démonstration

• Pour deux nombres entiers a et b, si a et b ont le même reste dans la division euclidienne par n, alors on a les égalités $a = nq + r$ et $b = nq' + r$.

Donc : $a - b = (nq + r) - (nq' + r) = nq + \cancel{r} - nq' - \cancel{r} = n(q - q')$.

Donc $a - b$ est multiple de n, par conséquent $a \equiv b\ [n]$.

• Réciproquement, si $a \equiv b\ [n]$, écrivons les divisions euclidiennes de a et b par n :

$a = nq + r$ et $b = nq' + r'$, avec $0 \leqslant r < n$ et $0 \leqslant r' < n$, et démontrons que $r = r'$.

On a : $a - b = nq + r - (nq' + r') = nq + r - nq' - r' = n(q - q') + r - r'$

Or, sachant que $0 \leqslant r' < n$, on a donc $-n < -r' \leqslant 0$, et par conséquent $-n < r - r' < n$.

▷ Si $r - r' \geqslant 0$, on a alors $0 \leqslant r - r' < n$.

Donc $r - r'$ est le reste de la division euclidienne de $a - b$ par n.

Or $a \equiv b\ [n]$, si bien que $a - b$ est multiple de n, donc le reste de la division euclidienne de $a - b$ par n est égal à zéro.

Donc $r - r' = 0$, donc $r = r'$, ainsi a et b ont le même reste dans la division euclidienne par n.

▷ Si $r - r' \leqslant 0$, alors $r' - r \geqslant 0$ et on procède de la même façon que précédemment avec $b - a$ au lieu de $a - b$, et la conclusion est la même.

Propriété 1.10 (Congruence et opérations)

Pour deux nombres entiers a et b, pour un nombre entier naturel $n \geqslant 2$, et pour un nombre entier naturel p, si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors
(1) $a + c \equiv b + d\ [n]$ **(2)** $a - c \equiv b - d\ [n]$ **(3)** $a \times c \equiv b \times d\ [n]$ **(4)** $a^p \equiv b^p\ [n]$

Exemple

$17 \equiv 8\ [3]$ et $10 \equiv 4\ [3]$.

(1) $(17 + 10) - (8 + 4) = 15$ et 15 est multiple de 3 donc $17 + 10 \equiv 19 + 22\ [3]$

(2) $(17 - 10) - (8 - 4) = 3$ et 3 est multiple de 3 donc $17 - 10 \equiv 8 - 4\ [3]$

(3) $17 \times 10 - 8 \times 4 = 138$ et $138 = 3 \times 46$ est multiple de 3 donc $17 \times 10 \equiv 8 \times 4\ [3]$

(4) $17^3 - 8^3 = 4401$ et $4\,401 = 3 \times 1\,467$ donc $17^3 \equiv 8^3\ [3]$

Démonstration

Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $a - b$ et $c - d$ sont multiples de n,
par conséquent, il existe des entiers k et k' tels que $a - b = kn$ et $c - d = k'n$,
donc : $a = b + kn$ et $c = d + k'n$.

On utilise alors ces deux égalités pour démontrer ci-dessous les propriétés (1), (2), (3).

(1) $a+c = b+kn+d+k'n = b+d+(k+k')n$ donc $(a+c)-(b+d) = (k+k')n$ donc $a+c \equiv b+d\ [n]$.

(2) $a - c = b + kn - (d + k'n) = b + kn - d - k'n = b - d + (k - k')n$

donc $(a - c) - (b - d) = (k - k')n$ donc $a - c \equiv b - d\ [n]$

(3) $a \times c = (b + kn) \times (d + k'n) = bd + kk'n + kdn + kk'n^2 = bd + n \times (kk' + kd + kk'n)$

donc $ac - bd = n \times (kk' + kd + kk'n)$, donc $ac - bd$ est multiple de n, donc $ac \equiv bd\ [n]$.

(4) On démontre cette égalité par récurrence sur p, en utilisant la propriété (3) pour l'hérédité.

1.3.b Exemple d'application

Utilisons tout ce que nous savons sur les congruences pour déterminer un reste dans une division euclidienne d'un grand nombre.

Énoncé : sans utiliser la calculatrice, déterminer le reste de la division euclidienne de $47\,000\,000\,000\,000\,000$ par 11.

Solution

$47\,000\,000\,000\,000\,000 = 47 \times 10^{15}$

Étudions les congruences de 47 et des puissances de dix modulo 11.

$47 = 11 \times 4 + 3$ donc $47 \equiv 3$ [11].

$10 \equiv -1$ [11] donc $10^2 \equiv (-1)^2 \equiv 1$ [11]

$10^{14} = (10^2)^7 \equiv 1^7 \equiv 1$ [11]

$10^{15} = 10^{14} \times 10 \equiv 1 \times 10 \equiv 10 \equiv -1$ [11]

$47\,000\,000\,000\,000\,000 = 47 \times 10^{15} \equiv 3 \times (-1) \equiv -3 \equiv 8$ [11]

Donc le reste de la division euclidienne de $47\,000\,000\,000\,000\,000$ par 11 est $\boxed{8}$.

1.4 Critères de divisibilité

Propriété 1.11

- Pour tout nombre divisible par 2, son chiffre des unités est 0 ou 2 ou 4 ou 6 ou 8.
- Pour tout nombre divisible par 3, sa somme des chiffres est un multiple de 3.
- Pour tout nombre divisible par 5, son chiffre des unités est 0 ou 5.