Divisibilité et congruence

Maths expertes

Année 2020-2021

Introduction

L'arithmétique, ayant pour objet l'étude des nombres entiers, est une des branches les plus élémentaires des mathématiques. Avec peu d'outils théoriques, on y démontre des résultats non triviaux. C'est aussi l'une des branches les plus difficiles et l'une des seules où des conjectures et des théorèmes dont l'étude théorique est redoutable peuvent être facilement énoncés.

I Les ensembles $\mathbb{N}$ et $\mathbb{Z}$

À l'occasion de ce paragraphe on répondra au problème suivant : le nombre $\sqrt{2}$ peut-il être exprimé comme le quotient de deux entiers ?

Définition (Ensembles des entiers naturels et relatifs)

On note $\mathbb{N}$ l'ensemble des entiers naturels :

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

et $\mathbb{Z}$ l'ensemble des entiers relatifs :

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Sur ces ensembles agissent des opérations bien connues comme l'addition et la multiplication. La question de savoir si le résultat d'une telle opération effectuée sur deux éléments d'un ensemble est encore dans cet ensemble est particulièrement importante. Heureusement on a la réponse :

Propriété (Stabilité des opérations)

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

Preuve : Admis. □

Remarque :

Les quotients font sortir a priori de $\mathbb{Z}$, par exemple 2 et 5 sont dans $\mathbb{Z}$ pourtant $\frac{2}{5} \notin \mathbb{Z}$.

Exercice 1

1. Déterminer deux entiers a et b tels que $\forall n \in \mathbb{Z}, n \neq -1$, $\dfrac{3n+8}{n+1} = a + \dfrac{b}{n+1}$.
2. Pour n un entier relatif différent de -1, montrer que $\dfrac{3n+8}{n+1}$ est un entier si et seulement si $\dfrac{5}{n+1}$ l'est.
3. En déduire les valeurs de n telles que $\dfrac{3n+8}{n+1}$ soit un entier.

Entraînement 1

Déterminer les valeurs de $n \in \mathbb{Z}$ tels que $\dfrac{2n+6}{n-1}$ soit dans $\mathbb{Z}$.

Définition (Nombres pairs, nombres impairs)

Les nombres pairs sont les entiers relatifs n de la forme $n = 2k$ avec $k \in \mathbb{Z}$.
Les nombres impairs sont les entiers relatifs n de la forme $n = 2k+1$ avec $k \in \mathbb{Z}$.

Remarque : Comment utiliser cette définition [1] ?

— Si **on sait** qu'un nombre m est impair alors on **dispose** d'une relation $m = 2k+1$ où $k \in \mathbb{Z}$.
— Si **on veut montrer** qu'un nombre p est pair alors il faut **produire** une relation du type $p = 2k$ en justifiant que k est dans $\mathbb{Z}$.
— Dans les deux cas, l'appartenance à l'ensemble $\mathbb{Z}$ est primordiale car son omission viderait de sens la relation. De plus elle ouvre la possibilité d'utiliser les propriétés de stabilité des opérations.

1. Ce sera la même chose pour les autres définitions de ce type

Exercice 2 : Montrer que la différence de deux carrés parfaits successifs est toujours impair.

Entraînement 2

Montrer que si on retire 1 au carré d'un nombre impair on obtient un multiple de 8.

Propriété (Parité et opération)

1. La somme de deux nombres de même parité est un nombre pair.
2. La somme de deux nombres de parités différentes est un nombre impair.
3. Le produit de deux nombres impairs est un nombre impair.
4. Le produit d'un nombre pair avec un nombre de parité quelconque est pair.

Preuve :

Entraînement 3

1. Faire les démonstrations qui n'ont pas été faites dans la preuve ci-dessus.
2. Montrer que pour tout $n \in \mathbb{N}$, le produit $P = n(n+1)$ est pair.

Exercice 3 : $\sqrt{2}$ est irrationnel

1. On souhaite prouver que $\sqrt{2}$ n'est pas un nombre rationnel. On raisonne par l'absurde en supposant que $\sqrt{2}$ est une fraction écrite sous forme irréductible : $\sqrt{2} = \frac{a}{b}$, en particulier a et b ne peuvent être tous deux pairs. Montrer que a^2 est pair, en déduire que a est pair.
2. Montrer que b et pair.
3. Conclure.

II Divisibilité dans $\mathbb{Z}$

Dans ce paragraphe, on définit les notions de diviseur et multiple. On établira un premier algorithme pour déterminer l'ensemble des diviseurs positifs d'un nombre donné. Enfin on appliquera ces notions à la résolution d'une famille d'équations diophantiennes.

Définition (Nombre divisible par)

Soient a et b dans $\mathbb{Z}$. On dit que a divise b (ou que b est divisible par a ou que b est un multiple de a) et on note $a \mid b$ lorsqu'il existe $k \in \mathbb{Z}$ tel que $ak = b$.

Remarques :

Le nombre k tel que $ak = b$ est lui aussi un diviseur de b, on dira que cet autre diviseur est associé à a. Attention le diviseur associé peut-être égal au diviseur (quand ?) [2].

Les multiples d'un entiers a sont les nombres de la forme ka où k est un entier relatif quelconque. On note cet l'ensemble : $a\mathbb{Z} = \{\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots\}$

Exercice 4

Montrer qu'un nombre qui s'écrit en décimal avec deux chiffres identiques est divisible par 11.

Entraînement 4

1. Soient a et b deux entiers. Montrer que $a^2 - b^2$ est divisible par $a + b$.
2. Un nombre de trois chiffres a son chiffre des dizaines qui est la somme des deux autres chiffres. Montrer qu'il est divisible par 11.

2. Lorsque b est un carré parfait.

Propriétés

1. Un nombre n non nul a ses diviseurs tous compris entre $-n$ et n.
2. Un entier non nul et son opposé ont tous les mêmes diviseurs.
3. Si a et b sont dans $\mathbb{Z}^*$ avec $a \mid b$ et $b \mid a$ alors $a = b$ ou $a = -b$.
4. Si a et b sont dans $\mathbb{N}^*$ avec $a \mid b$ et $b \mid a$ alors $a = b$.
5. Pour a, b, c et d quelconques dans $\mathbb{Z}$,
   (a) si $a \mid b$ alors $a \mid bc$,
   (b) si $a \mid b$ et $c \mid d$ alors $ac \mid bd$,
   (c) si $c \in \mathbb{Z}^*$ et $ac \mid bc$ alors $a \mid b$,
   (d) si $a \mid b$ et $b \mid c$ alors $a \mid c$,
   (e) si $a \mid b$ et $a \mid c$ alors $a \mid b + c$ et $a \mid b - c$,
   (f) si $a \mid b$ et $a \mid c$ alors pour tout $u, v \in \mathbb{Z}$, $\quad a \mid bu + cv$.

Remarques :

On dit que $bu + cv$ est une combinaison linéaire de b et c à coefficients dans $\mathbb{Z}$.

Preuve :

Entraînement 5

Faire les démonstrations qui n'ont pas été faites dans la preuve ci-dessus.

Exercice 5

Soit n un entier relatif, montrer que si un entier relatif a divise $2n + 5$ et $3n + 4$, alors a divise 7. Quelles sont alors les valeurs possibles de a ?

Définition (Ensemble des diviseurs d'un nombre)

Pour un entier relatif a donné on note $\mathcal{D}_{\mathbb{Z}}(a)$ l'ensemble des entiers relatifs n tels que $n \mid a$, c'est l'ensemble des diviseurs de a.

Pour un entier naturel b donné on note $\mathcal{D}_{\mathbb{N}}(b)$ l'ensemble des entiers naturels n tels que $n \mid b$, c'est l'ensemble des diviseurs positifs de b.

Les ensembles $\mathcal{D}_{\mathbb{Z}}(a)$ et $\mathcal{D}_{\mathbb{N}}(b)$ sont des ensembles finis pourvu que a et b soient non nuls.

Exercice 6 : Déterminer $\mathcal{D}_{\mathbb{Z}}(25)$ puis $\mathcal{D}_{\mathbb{N}}(15)$

Pour déterminer pratiquement ces ensembles on dispose de :

Propriété (Détermination pratique de l'ensemble des diviseurs)

- Pour a un entier relatif non nul $\mathcal{D}_{\mathbb{Z}}(a)$ est constitué des éléments de $\mathcal{D}_{\mathbb{N}}(|a|)$ et de leurs opposés.
- Si k et k' sont deux diviseurs associés d'un entier naturel non nul a avec $k \leq k'$ alors $k^2 \leq a$.

Preuve :

Pour déterminer l'ensemble $\mathcal{D}_{\mathbb{N}}(a)$ on teste les entiers les uns après les autres en commençant par 1, on note les diviseurs avec leur diviseur associé et on s'arrête lorsque le carré du nombre testé dépasse a.

Exercice 7

Déterminer $\mathcal{D}_{\mathbb{N}}(51)$ puis $\mathcal{D}_{\mathbb{N}}(165)$

Remarque : On a programmé lors du TD Algorithmique la fonction Python correspondante.

Application de la divisibilité : les équations diophantiennes « factorisables »

Une équation diophantienne est une équation dont on recherche les solutions en nombres entiers uniquement. Si on peut la mettre sous la forme d'un produit de deux entiers égalisé à un nombre donné alors les facteurs forment un couple de diviseurs associés de ce nombre.

Exercice 8 : Résoudre $4x^2 = y^2 + 7$ dans $\mathbb{N}$.

Entraînement 6

Résoudre $a^2 - b^2 = a + 2$ dans $\mathbb{Z}$.

Indication : On commencera par prouver que si (a, b) *est solution alors* $(2a - 2b - 1)(2a + 2b - 1) = 9$.

III Division euclidienne

Dans $\mathbb{N}$ et $\mathbb{Z}$ on peut calculer mais on peut aussi comparer les nombres entre eux à l'aide de la relation $\leq$. Ainsi $2 \leq 5$, $-3 \leq 4$, $12 \leq 12$ et $2n \leq n^2 + 1$ sont vraies tandis que $4 \leq 0$ ne l'est pas. On utilisera en particulier les propriétés suivantes :

Propriétés

1. (Antisymétrie) : $\forall a, b \in \mathbb{Z}$ si $a \leq b$ et $b \leq a$ alors $a = b$.
2. (Transitivité) : $\forall a, b, c \in \mathbb{Z}$ si $a \leq b$ et $b \leq c$ alors $a \leq c$.
3. Tout sous-ensemble non-vide de $\mathbb{N}$ admet un plus petit élément.
4. Tout sous-ensemble non-vide et majoré de $\mathbb{N}$ admet un plus grand élément.

Preuve : Admis. □

Ces propriétés appellent plusieurs remarques et commentaires :
— La propriété d'antisymétrie permet de montrer des égalités à l'aide de deux inégalités ainsi l'ordre peux intervenir dans des raisonnements où on ne l'attend pas a priori.
— Le plus petit élément d'un ensemble E est un élément e de E tel que pour tout x de E on ait $e \leq x$, il est unique. On a une définition analogue pour le plus grand élément.
— La propriété 3 permet souvent de résoudre des problèmes d'existence. Attention, elle est fausse dans $\mathbb{Z}$ ou dans $\mathbb{R}_+$.
— La relation $<$ est relié à $\leq$ par $x < y \Leftrightarrow (x \leq y \text{ et } x \neq y)$. Il en est de même pour $>$.

Propriété-Définition (Division euclidienne)
Soit a un entier relatif quelconque et b un entier naturel non nul, il existe un unique couple d'entier relatif (q, r) tel que

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

On dit alors que q est le quotient de la division et r son reste.

Interprétation : Il s'agit d'encadrer a par deux multiples consécutifs de b, le reste donnant l'écart au plus petit des deux. Faisons une figure pour en avoir une vision géométrique :

Preuve :

Exercice 9

Déterminer les divisions euclidiennes de : (a) 137 par 11 (b) 114 par 8 (c) -228 par 15

On rappelle qu'en **Python** le quotient de la division euclidienne s'obtient par `a//b` et le reste par `a%b`.

Sur la **calculatrice**, le quotient de a par b s'obtient par le plus grand entier inférieur au résultat de la division décimal $a \div b$. Le reste est alors $r = a - bq$.

Exercice 10

Si la division de a par b donne un quotient q et un reste r. Pour $k \in N^*$, que dire de la division de ka par kb ?

Entraînement 7

Soient a et b deux nombres entiers naturels non nuls. Les entiers q et r sont respectivement le quotient et le reste dans la division euclidienne de a par b.

Exprimer en fonction des données le reste et le quotient de la division euclidienne de $-a$ par b (il faudra distinguer selon que $r = 0$ ou $r \neq 0$).

IV Congruence

Avec la notion de nombre pair et impair on a vu que les entiers relatifs se répartissaient en deux classes et ce, de manière compatible avec les opérations usuelles (la parité de la somme de dépend que de celles des deux termes, de même pour le produit). Les congruences généralisent cette situation en répartissant les relatifs en un nombre quelconque de classes.

Définition (Entiers congrus modulo m)

Soit m un entier naturel non nul. On dit que les relatifs a et b sont congrus modulo m lorsqu'ils ont même reste dans la division euclidienne modulo m. On note alors $a \equiv b\ [m]$

Remarque :

Dans le cas où $m = 2$, les seuls restes possibles sont 0 ou 1, dans le premier cas on a les nombres pairs et dans le second les impairs ; on retrouve la classification due à la parité.

Propriété

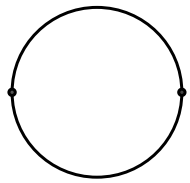
1. $a \equiv b\ [m]$ si et seulement si m divise $b - a$.
2. $a \equiv b\ [m]$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $b = a + km$.
3. $a \equiv b\ [m]$ si et seulement si $b \equiv a\ [m]$.
4. Si $a \equiv b\ [m]$ et $b \equiv c\ [m]$ alors $a \equiv c\ [m]$.
5. $a \equiv r\ [m]$ et $0 \leq r < m$ si et seulement si r est le reste de la division euclidienne de a par m.

Remarques :

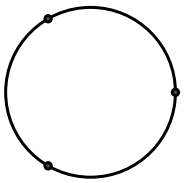
— Un entier relatif est toujours congru modulo m à son reste de la division par m, ainsi il n'y a que m cas à envisager pour mener un raisonnement par distinction de cas : nombres congru à 0, 1, 2, ..., $m-1$. On présentera souvent de tels raisonnements par distinction de cas **à l'aide d'un tableau.**

— On obtient les nombres congrus à 0 modulo m en comptant de m en m en partant de 0 (dans le sens croissant et aussi 'à rebours'), les nombres congrus à 1 en partant de 1, les nombres congrus à 2 en partant de 2,.. etc.

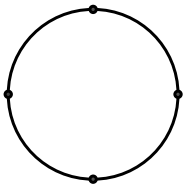
— Pour avoir une bonne idée géométrique de cette situation on place les entiers autour du cercle unité [3] :



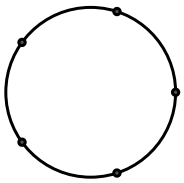
Les relatifs modulo 2



Les relatifs modulo 3



Les relatifs modulo 4



Les relatifs modulo 5

Preuve :

3. On retrouvera ces figures lors de l'étude des racine n-ième de l'unité dans un prochain chapitre.

Propriété (Congruence et opérations)

Si $a \equiv b\ [m]$ et $c \equiv d\ [m]$ alors

- $a + c \equiv b + d\ [m]$,
- $a - c \equiv b - d\ [m]$,
- $ac \equiv bd\ [m]$.
- Pour tout k entier naturel, $a^k \equiv b^k\ [m]$.

Remarques :

— Pour résumer ; on peut additionner, soustraire, multiplier ou élever à une même puissance des congruences de même module.

— On ne peut pas simplifier une congruence comme une égalité : si $ac \equiv bc\ [m]$ on ne peut pas conclure en général que $a \equiv b\ [m]$, comme le montre le contre exemple :

— Dans le cas où l'on peut trouver un 'inverse en congruence' à c, c'est à dire un nombre d tel que $cd \equiv 1\ [m]$ alors la simplification est possible, on procédera dans les exercices au cas par cas en utilisant, par exemple, le théorème de Bezout ou celui de Gauss [4].

— Les congruences ne passent pas aux exposants : si $p \equiv q\ [m]$ on ne peut pas conclure que $a^p \equiv a^q\ [m]$ (ce sera même très généralement faux), voir le contre-exemple suivant :

Preuve :

---

4. Vus dans un chapitre à venir

Exercice 11 : La 'preuve' par 9

La preuve par neuf est une méthode de vérification des calculs faits à la main bien connue de nos grands-parents. On souhaite vérifier un calcul (somme, différence ou produit) effectué entre deux nombres a et b. On calcule la somme des chiffres qui composent a et b (en recommençant si on obtient une somme plus grande que 9), on effectue la même opération que celle que l'on souhaite vérifier sur les deux nombres obtenus puis on compare avec la somme des chiffres du résultat. Si on obtient des chiffres différents le calcul est faux, si ils sont identiques il y a 8 chances sur 9 que le calcul soit exact.

1. Mettre en oeuvre la preuve par neuf pour vérifier ou infirmer le calcul $71 \times 82 = 5722$.
2. Montrer qu'un nombre a écrit sous forme décimal $A_n A_{n-1} \dots A_1 A_0$ est congru modulo 9 avec la somme de ses chiffres $s = A_n + A_{n-1} + \dots + A_1 + A_0$.
3. Expliquer le fonctionnement de la preuve par 9.

Exercice 12

1. Déterminer le reste de la division euclidienne de 23^{41} par 7.
2. Montrer que $1^{2015} + 2^{2015} + 3^{2015} + 4^{2015}$ est divisible par 5.

Entraînement 8

Montrer que pour tout entier naturel n non nul $3^{2n} - 1$ est divisible par 8.

Propriété (Congruence dans les expressions polynomiales)

Soit P est un polynôme à coefficients dans $\mathbb{Z}$ et m un entier naturel non nul.

Pour tout $n \in \mathbb{Z}$, le reste de la division euclidienne de $P(n)$ par m ne dépend que de celui de n par m.

Autre formulation : Pour tous a et b dans $\mathbb{Z}$, si $a \equiv b\ [m]$ alors $P(a) \equiv P(b)\ [m]$.

Preuve :

Exercice 13

1. Résoudre dans $\mathbb{Z}$, l'équation diophantienne $2x^2 - y^2 = 5$.
2. Déterminer les entiers n tels que $2^n - 1$ est divisible par 9.

Remarque : les exercices de congruence où la variable/inconnue intervient à l'exposant se résolve de manière très différente des autres, on aura intérêt à ne pas confondre les différentes situations ...