ARITHMÉTIQUE DANS Z

1.0

ATIAMPO KODJO ARMAND@ UVCI
2017

1

Table des matières

Objectifs

À la fin de cette leçon, vous serez capable :

- **Comprendre** l'arithmétique des nombres entiers notamment la division euclidienne ;
- **Manipuler** les notions de PGCD, de PPCM et de nombre premier
- **Résoudre** les équations algébriques.

Introduction

Cette leçon présente les concepts de base de l'arithmétique et va nous permettre d'illustrer les raisonnements présentés des précédentes leçons. Les notions présentées trouvent leur usage dans la résolution d'équation et dans la conception d'algorithme de calcul.

Division Euclidienne

I

Objectifs

A la fin de ceste section , l'étudiant sera capable de :

- **Identifier** les nombres premiers
- **Manipuler** la division euclidienne dan Z

Il s'agit de formaliser avec précision la bonne vieille division euclidienne, celle que vous connaissez depuis l'école primaire.

A. Divisibilité

On appelle entier (ou entier relatif, c'est-à-dire positif ou négatif) tout élément de Z = { . . . , −3, −2, −1, 0, 1, 2, 3,....}

Soient d et n des entiers naturels. On dit que **d divise n** et on note **d|n si ∃k ∈ N, n = dk.**

On dit aussi que d est un diviseur de n et que **n est un multiple de d.**

Exemple

6= 2×3. on en déduit que 2 divise 6(resp. 3 divise 6) et 6 est un multiple de 2 (resp. de 3)

On appelle nombre premier tout nombre entier naturel ayant exactement **deux diviseurs : 1 et lui-même.**

Exemple

2, 3, 5, 7, 11, ... sont des nombres premiers car ils n'ont aucun diviseur à part eux-mêmes et 1

Attention

1 n'est pas un nombre premier

Définition

Soient a et b des entiers naturels avec $b \neq 0$. **Il existe un unique couple d'entiers $(n, r) \in \mathbb{N} \times \mathbb{N}$**

tel que $a = nb + r$ et $0 \leq r < b$.

Cette égalité est appelée division euclidienne de a par b ; n est le quotient de la division et r en est le reste.

Définition

On dit que deux entiers naturels a et b sont **premiers entre eux** s'ils **n'ont aucun diviseur commun hormis 1 :**

$\forall d \in \mathbb{N}, (d|a \text{ et } d|b) \Longrightarrow d = 1.$

Exemple

Les entiers 14 et 15 sont premiers entre eux. En effet l'ensemble des diviseurs de 14 est l'ensemble A={-14, -7, -2, 1, 2, 7, 14}. L'ensemble des diviseurs de l'entier 15 est B={-15, -5, -3, 1, 3, 5, 15}. Comme on le voit 15 ni 15 ne sont des nombres premiers mais ils sonr premiers entre eux car leur seul diviseur commun est 1

B. Exercice

[Solution n°1 p 27]

Parmi les assertions suivantes , lesquelles sont vérifiées ?

- [ ] -3 est un nombre premier
- [ ] Un nombre premier est un nombre impair
- [ ] L'ensemble des diviseurs de 3 est {-3, -1, 3, 1}
- [ ] L'ensemble des nombres premiers est un ensemble fini
- [ ] Les entiers 14 et 35 sont premiers entre eux
- [ ] Soient a et b deux entiers premiers entre eux alors a ou b est un nombre premier

C. Exercice

[Solution n°2 p 27]

Parmi les assertions suivantes , lesquelles sont vérifiées

- ☐ La relation "divise" n'est pas une relation d'ordre dans Z
- ☐ La relation "divise" est une relation d'ordre dans N
- ☐ La relation "divise " est transitive dans Z
- ☐ Aucune des affirmations précédentes n'est vraie

PGCD, PPCM

II

Objectifs

A la fin de cette section, l'étudiant sera capable de :

- **Identifier** le pgcd de deux nombres entiers
- **Identifier** le ppcm de deux nombres entiers
- **Manipuler** l'identité de Bézout

Dans cette section, nous allons étudier les propriétés élémentaires des nombres entiers qui nous serviront de base pour la résolution d'équations algébrique. Nous n'allons pas effectuer les démonstrations des théorèmes , mais le lecteur curieux est invité à chercher à les faire pour mieux appréhender les contours et améliorer la maîtrise des concepts étudies dans les chapitres précédents

A. PGCD et PPCM

Définition

On appelle **plus grand commun diviseu**r (PGCD) de deux entiers a et b **le plus grand nombre entier naturel qui divise à la fois a et b :**

$d = PGCD(a, b)$ si $d|a$ et $d|b$ et $(\forall d' \in N, d'|a \text{ et } d'|b \Longrightarrow d'|d)$.

Définition

Soit $a \geq 1$ et $b \geq 1$ deux entiers. Alors il existe un unique entier $m \geq 1$ tel que pour tout entier $c \geq 1$,

c est un multiple de a et de b si et seulement si c est un multiple de m.

m est alors le plus petit commun multiple des entiers a et b. **On le note m=PPCM(a,b)**

Fondamental: Identité de Bézout

Soient a et b deux entiers naturels premiers entre eux. Alors il existe des entiers relatifs u et v tels que

$au + bv = 1$.

Il existe une version forte de ce résultat qui le généralise au cas où les nombres ne sont pas premiers entre eux

Fondamental

$\forall a \in \mathbb{N}$, $\forall b \in \mathbb{N}$, $\exists u \in \mathbb{Z}$, $\exists v \in \mathbb{Z}$, $au + bv = \text{PGCD}(a, b)$.

L'algorithme d'Euclide permet de déterminer ce PGCD et de trouver des coefficients u et v vérifiant l'égalité de Bézout et sa version forte.

Complément : Lemme d'Euclide

Soit p un nombre premier et soient $a, b \in \mathbb{N}$. Si p divise le produit ab, alors p divise a ou p divise b :

$\forall p \in P$, $\forall (a, b) \in \mathbb{N} \times \mathbb{N}$, $p|ab \Longrightarrow p|a$ ou $p|b$.

Méthode

Programme de calcul des coefficients u et v de l'identité de Bézout

Début du programme

*** pgcd (a, 0) = a.**

*** Soit r le reste de la division euclidienne de a par b.**

Les diviseurs communs de a et b sont les diviseurs communs de b et r.

D'où : pgcd (a, b) = pgcd (b, r).

Fin du programme

Exemple

Calculons le pgcd de 137 et 24 . En appliquant le lemme d'Euclide , nous avons

(1) $137 = 5 \times 24 + 17$ pgcd(137, 24) = pgcd(24, 17)

(2) $24 = 1 \times 17 + 7$ pgcd(24, 17) = pgcd(17, 7)

(3) $17 = 2 \times 7 + 3$ pgcd(17, 7) = pgcd(7, 3)

(4) $7 = 2 \times 3 + 1$ pgcd(7, 3) = pgcd(3, 1)

(5) $3 = 3 \times 1 + 0$ pgcd(3, 1) = pgcd(1, 0) = 1

Donc pgcd(137, 24) = 1.

Ces calculs permettent ensuite sans mal de reconstituer une identité de Bézout.

– La dernière division avec un reste non nul est (4) qui donne $1 = 7 - 2 \times 3$.

On va repêcher une expression de 3 comme un reste dans la relation précédente, soit (3), ce qui donne $3 = 17 - 2 \times 7$.

– On reporte cette expression de 3 donc $1 = 7 - 2 \times (17 - 2 \times 7)$.

– On regroupe les termes en 17 et 7 donc $1 = -2 \times 17 + 5 \times 7$.

– On va repêcher une expression de 7 comme un reste dans la relation précédente, soit (2), ce qui donne $7 = 24 - 1 \times 17$.

– On reporte cette expression de 7 donc $1 = -2 \times 17 + 5 \times (24 - 1 \times 17)$.

– On regroupe les termes en 24 et 17 donc $1 = 5 \times 24 - 7 \times 17$.

– On va repêcher une expression de 17 comme un reste dans la relation précédente, soit (1), ce qui donne $17 = 137 - 5 \times 24$.

– On reporte cette expression de 17 donc $1 = 5 \times 24 - 7 \times (137 - 5 \times 24)$.

– On regroupe les termes en 137 et 24 donc

$1 = -7 \times 137 + 40 \times 24$.

Exemple

On va déterminer le pgcd de 141 et 24

A partir du lemme d'Euclide , nous avons les calculs suivants

Voici les divisions euclidiennes successives et leurs conséquences en termes de pgcd.

(1) $141 = 5 \times 24 + 21$, pgcd (141, 24) = pgcd (24, 21)

(2) $24 = 1 \times 21 + 3$, pgcd (24, 21) = pgcd (21, 3)

(3) $21 = 7 \times 3 + 0$, pgcd(21, 3) = pgcd(3, 0) = 3

Donc pgcd (141, 24) = 3 et on vérifiera que ces calculs permettent de reconstituer l'identité de Bézout

$-141 + 6 \times 24 = 3$.

Conseil : On part de l'équation (2) et on remonte à l'expression (1) pour trouver la dernière égalité

Fondamental : Lemme de Gauss

Soit a, b et c trois entiers strictement positifs. Si a divise le produit bc et si a est premier avec c, alors a divise b.

Fondamental : Théorème fondamental de l'arithmétique

Tout nombre entier naturel non nul se décompose en un produit fini de nombres premiers :

$$\forall n \in \mathbf{N}^*, \exists k \in \mathbf{N}, \exists p_1, \dots, p_k \in \mathcal{P},\ n = \prod_{i=1}^{k} p_i.$$

Cette décomposition est unique à l'ordre des facteurs près

$\mathcal{P}$ est l'ensemble des nombres premiers

Fondamental

Soient m et n deux entiers alors on a le résultat suivant pgcd(m,n) ppcm(m,n)=mn

Exemple

Déterminer toutes les solutions dans $\mathbb{Z} \times \mathbb{Z}$ de l'équation : $7x + 5y = 3$

Solution

Il faut remarquer que 7 et 5 sont premiers entre eux. Nous allons donc utiliser l'algorithme d'Euclide

$7 = 1 \times 5 + 2$

$5 = 2 \times 2 + 1$

$2 = 2 \times 1 + 0$

Donc $1 = 5 - 2 \times 2 = 5 - 2 \times (7 - 1 \times 5) = -2 \times 7 + 3 \times 5$

On multiplie cette égalité par 3 : $-6 \times 7 + 9 \times 5 = 3$. On soustrayant $7x + 5y = 3$ et $-6 \times 7 + 9 \times 5 = 3$ on

trouve que : $7(x + 6) + 5(y - 9) = 0$, ce qui équivaut à $7(x + 6) = -5(y - 9)$,

d'après le lemme de
Gauss, 7 divise $5(y - 9)$ et pgcd(7 , 5)= 1 donc 7 divise $y - 9$, il existe donc $k \in \mathbb{Z}$ tel que :
$y - 9 = 7k$, ce que je remplace dans $7(x + 6) = -5(y - 9)$ ce qui donne $7(x + 6) = -5 \times 7k$, puis en
simplifiant par 7 : $x + 6 = -5k$.
L'ensemble des solution est ?? = $\{(-6 - 5k, 9 + 7k), k \in \mathbb{Z}\}$

B. Exercice

[*Solution n°3 p 27*]

Exercice

Soient a et b deux entiers quelconques.

- [ ] Si a divise b, alors pgcd(a, b) = a.
- [ ] Si un nombre divise ppcm(a, b), alors il divise a ou b.
- [ ] Si b = pgcd(a, b) × a alors b = a × a.
- [ ] Si axa = pgcd(a, b) × b, alors a × a = b.
- [ ] Si ppcm (a, b) × a divise ab alors b = 1.

Exercice

Soient a, b, d trois entiers.

- [ ] S'il existe 2 entiers u et v tels que au + bv = d, alors d = pgcd(a, b).
- [ ] S'il existe 2 entiers u et v tels que au + bv = d, alors d divise a et b.
- [ ] S'il existe 2 entiers u et v tels que au + bv = d, alors tout diviseur commun de a et b divise d.
- [ ] Si d = pgcd(a, b), alors il existe un couple unique d'entiers (u, v) tel que au + bv = d.
- [ ] Si a et b sont premiers entre eux, alors pour tout entier k, il existe deux entiers u et v tels que au + bv = dk

Congruences

III

Objectifs

A la fin de cette section l'étudiant sera capable de :

- **Identifier** le sous-groupe Z/nZ
- **Résoudre** les équations algébriques dans l'ensemble Z/nZ

Dans cette section, nous allons utiliser les résultats préalablement établis afin d'étudier un ensemble particulier Z/nZ. La résolution d'équations dans ce ensemble trouve des applications en cryptologie

A. Congruences

Soit b un entier. On note **bZ** l'ensemble des multiples de b.

Fondamental

Les sous-groupes de Z sont exactement les **ensembles bZ** avec $b \geq 0$.

Exemple

le sous-groupe de Z engendré par 3 est A=<3>={3k| k∈ Z}={..., -9, -6, -3,0, 3, 6, 9, 12,...}

Définition

Soit a et b des entiers relatifs et $n \geq 1$ un entier strictement positif. On dit que **a est congru à b modulo n**

lorsque **b − a est un multiple de n.**

On note **a ≡ b mod n** ou encore **a ≡ b[n]**.

Complément

Avec les mêmes notations, a est congru a b modulo n si a est égal à b à un multiple de n près :

a ≡ b[n] ssi ∃ k ∈ Z, a = b + kn.

Fondamental: Proposition

Soit $n \geq 1$ fixé et soit a, b et c trois entiers relatifs. Alors :

si $a \equiv b$ [n] alors $a + c \equiv b + c$ [n] et $ac \equiv bc$ [n].

Exemple

On repère les jours de l'année par leur numéro de 1 à 365 ou 366 selon les cas. Alors les numéros de tous les lundis sont congrus les uns aux autres modulo 7.

Exemple

Quel est le reste de la division par 9 de 12345 ? On commence par écrire

$12345 = 104 + 2 \cdot 103 + 3 \cdot 102 + 4 \cdot 10 + 5.$

Comme $10 \equiv 1$ [9] puisque $10 - 1 = 9$, on en déduit

$123456 \equiv 14 + 2 \cdot 13 + 3 \cdot 12 + 4 \cdot 1 + 5 = 1 + 2 + 3 + 4 + 5 = 15,$

et

$12345 \equiv 1 \cdot 10 + 5 \equiv 1 \cdot 1 + 5 = 1 + 5 = 6,$

donc la réponse est 6. par la suite o n note que $12345 \equiv 6[9]$

De me^me il est facile de voir que $12345 \equiv 3[11]$ en utilisant le fait que $10 \equiv -1$ [11]

Syntaxe

Soit $n \in Z$ et $a \in Z$. On note $\overline{a}$ l'ensemble des entiers congrus à a modulo n :

$\overline{a} = \{a + kn \mid k \in Z\} = \{. . . a - 3n, a - 2n, a - n, a, a + n, a + 2n, . . .\}=cl(a).$

Cet ensemble est appelé classe de congruence modulo n de a.

B. Exercice

[Solution n°4 p 28]

Parmi les assertions suivantes , lesquelles sont vérifiées ?

- [ ] la relation de congruence dans N est une relation d'équivalence.
- [ ] la relation de congruence dans Z est une relation d'équivalence.
- [ ] la relation de congruence dans Z est une relation d'ordre
- [ ] Aucune des assertions précédentes n'est vraie

C. Exercice

[Solution n°5 p 29]

Parmi les affirmations suivantes, lesquelles sont vraies ?

- ☐ Si un entier est congru à 0 modulo 6, alors il est divisible par 6
- ☐ Si le produit de deux entiers est congru à 0 modulo 6 alors l'un des deux est multiple de 6.
- ☐ Si un entier est congru à 5 modulo 6 alors toutes ses puissances paires sont congrues à 1 modulo 6.
- ☐ Si deux entiers sont congrus à 4 modulo 6, alors leur somme est congrue à 2 modulo 6.
- ☐ Si deux entiers sont congrus à 4 modulo 6, alors leur produit est congru à 2 modulo 6
- ☐ Si un entier est congru à 4 modulo 6 alors toutes ses puissances sont aussi congrues à 4 modulo 6.

D. Z/nZ

Fondamental

Soient n, a et b des entiers tels que a ≡ b mod n. Alors $\bar{a} = \bar{b}$

On dit que a et b sont des représentants de la classe de congruence .

Si n 6= 0, l'ensemble Z est l'union disjointe des classes de congruence cl(0), cl(1),...,cl(n-1)

$$\mathbf{Z} = \bigsqcup_{k=0}^{n-1} \bar{k}.$$

On note Z/nZ l'ensemble des classes de congruence modulo n

$$\mathbf{Z}/n\mathbf{Z} = \{\bar{k}\ ;\ k = 0 \ldots n-1\} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}.$$

Exemple

Considérons l'anneau Z/5Z. Si nous le définissons en extension alors Z/5Z ={cl(0), cl(1), cl(2), cl(3),cl(4)} ou encore en utilisant une notation moins lourde

$$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

La table de vérité pour l'addition est :

$\bar{+}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

la table de vérité pour la multiplication

$\bar{\times}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	1	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Soit cl(a) et cl(b) deux éléments de Z/nZ.
On définit la somme de cl(a) et cl(b) par
cl(a) + cl(b) = cl(a + b)
et leur produit par
cl(a) × cl(b) = cl(ab).

$$\forall \bar{a}, \bar{b} \in \mathbf{Z}/n\mathbf{Z} \quad \bar{a} \bar{+} \bar{b} = \overline{a+b} \text{ et } \bar{a} \bar{\times} \bar{b} = \overline{ab}.$$

Remarque

Remarque : plutôt qu'écrire $3+6 \equiv 2 \mod 7$, *on préfère écrire : dans* $\mathbf{Z}/7\mathbf{Z}$, $\bar{3} \bar{+} \bar{6} = \bar{2}$. *Et lorsque le contexte est clair, on ne note plus les éléments et les opérations de* $\mathbf{Z}/n\mathbf{Z}$ *avec des barres.*

Conseil

Une façon intuitive de calculer cl(a)+cl(b) est de calculer la somme de a+b et de lui associer le reste de la division euclidienne par n. <par exemple dans Z/5Z cl(4)+ cl(3) = cl(7)=cl(2) car 7 =1 × 5 +2

On applique un raisonnement semblable pour la multiplication

Fondamental

Pour tout n ≥ 1, Z/nZ est un anneau commutatif pour l'addition des classes et pour la multiplication des classes.

Fondamental

Pour tout n ≥ 1, **Z/nZ est un corps commutatif** si et seulement si **n est un nombre premier**.

Résolution des équations algébriques

Résoudre dans Z l'équation suivante, d'inconnue x :

$24x + 5 \equiv 0\ [137]$.

La restitution de cette équation peut se faire de deux façons possibles

Première résolution (sans Z/137Z)

Remarquons que 137 est premier, et donc que 137 et 24 sont premiers entre eux ; cherchons à écrire une identité de Bézout entre 137 et 24 ; en utilisant l'algorithme d'Euclide , on découvre que :

$1 = 40 \times 24 - 7 \times 137$,

d'où on déduit (par une simple multiplication par 5) que :

$5 = 200 \times 24 - 35 \times 137$.

Reportons cette identité dans l'équation, qui devient donc :

$24x + 200 \times 24 - 35 \times 137 \equiv 0\ [137]$.

À son tour, cette équation est équivalente à la condition suivante :

$24(x + 200) \equiv 0\ [137]$

qui signifie que 137 divise $24(x + 200)$, donc, en utilisant le lemme de Gauss puisque 137 et 24 sont premiers entre eux, que 137 divise $x + 200$. Finalement, x est solution si

et seulement si $x + 200 \equiv 0\ [137]$, c'est-à-dire $x \equiv -200\ [137]$, c'est-à-dire $x \equiv 74\ [137]$.

Deuxième résolution (avec Z/137Z)

Remarquons que 137 est premier, et donc que Z/137Z est un corps commutatif.

Faisons tous les calculs dans ce corps.

L'équation proposée se réécrit $cl(24)cl(x) + cl(5) = cl(0)$, soit $cl(24)cl(x) = -cl(5)$,

soit $cl(x) = -cl(5)(cl(24))^{-1}$

Calculons donc $(cl(24))^{-1}$; pour cela nous connaissons la bonne méthode : écrire une identité de Bézout entre 24 et 137, à savoir

$1 = 40 \times 24 - 7 \times 137$,

puis redescendre aux classes d'équivalence dans Z/137Z : $cl(1) = cl(40) \cdot cl(24)$, soit :

$(cl(24))^{-1} = cl(40)$.

On en conclut que l'équation proposée équivaut à :

$cl(x) = -cl(5)(cl(24))^{-1} = -cl(5) \times cl(40) = -cl(200) = cl(74)$

Exemple

Résoudre dans Z l'équation suivante, d'inconnue x : $x^4 \equiv 81\ [73]$.

Nous allons utiliser l'ensemble Z/73Z

Tout d'abord, l'équation s'écrit $x^4 - 81 \equiv 0\ [73]$ et, dans Z,

$x^4 - 81 = (x^2 - 9)(x^2 + 9) = (x - 3)(x + 3)(x^2 + 9)$.

Dans Z/73Z, l'équation s'écrit donc

$(cl(x) - cl(3))(cl(x) + cl(3))(cl(x)^2 + cl(9)) = cl(0)$

Mais $cl(9) = -cl(64)$ donc

$cl(x)^2 + cl(9) = cl(x)^2 - cl(64) = (cl(x) - cl(8))(cl(x) + cl(8))$.

Finalement, en utilisant cl(8) = −cl(65) et cl(3) = −cl(70), on voit que l'équation de départ s'écrit
(cl(x) − cl(3))(cl(x) − cl(70))(cl(x) − cl(8))(cl(x) − cl(65)) = cl(0),
soit cl(x) = cl(3) ou cl(x) = cl(8) ou cl(x) = cl(65) ou cl(x) = cl(70), car Z/73Z est un corps commutatif, donc intègre.
Les solutions de l'équation proposée sont donc
x ≡ 3 [73] ou x ≡ 8 [73] ou x ≡ 65 [73] ou x ≡ 70 [73].

E. Exercice

[Solution n°6 p 29]

Parmi ls réponses suivantes laquelle est la solution de l'équation algébrique suivante Résoudre dans Z l'équation suivante, d'inconnue x :
x17 ≡ 3 [19]

- ◯ x ≡ 17 [19].
- ◯ x ≡ 13 [19].
- ◯ x ≡ 1 [19].
- ◯ x ≡ 15 [19].

F. Exercice

[Solution n°7 p 30]

Dans l'anneau Z/12Z, combien d'éléments vérifient x2 = 1 ?

- ☐ 1
- ☐ 2
- ☐ 4
- ☐ Une infinité

Conclusion

Cette leçon nous a permis de disposer d'un cadre plus formel de l'ensemble des règles de bases de l'arithmétique dans Z. ces notions seront utilisés dans beaucoup de domaines notamment en sécurité informatique lors de la construction d'algorithmes de cryptage. Ci-joint un lien de court pour aller plus loin.

1-arith.pdf (cf.)

Solution des exercices

> Solution n°1 (exercice p. 10)

☐	-3 est un nombre premier
☑	Un nombre premier est un nombre impair
☑	L'ensemble des diviseurs de 3 est {-3, -1, 3, 1}
☐	L'ensemble des nombres premiers est un ensemble fini
☐	Les entiers 14 et 35 sont premiers entre eux
☐	Soient a et b deux entiers premiers entre eux alors a ou b est un nombre premier

> Solution n°2 (exercice p. 11)

☑	La relation "divise" n'est pas une relation d'ordre dans Z
☑	La relation "divise" est une relation d'ordre dans N
☐	La relation "divise " est transitive dans Z
☐	Aucune des affirmations précédentes n'est vraie

> Solution n°3 (exercice p. 16)

Exercice

- [x] Si a divise b, alors pgcd(a, b) = a.
- [ ] Si un nombre divise ppcm(a, b), alors il divise a ou b.
- [x] Si b = pgcd(a, b) × a alors b = a × a.
- [ ] Si axa = pgcd(a, b) × b, alors a × a = b.
- [ ] Si ppcm (a, b) × a divise ab alors b = 1.

Exercice

- [ ] S'il existe 2 entiers u et v tels que au + bv = d, alors d = pgcd(a, b).
- [ ] S'il existe 2 entiers u et v tels que au + bv = d, alors d divise a et b.
- [x] S'il existe 2 entiers u et v tels que au + bv = d, alors tout diviseur commun de a et b divise d.
- [ ] Si d = pgcd(a, b), alors il existe un couple unique d'entiers (u, v) tel que au + bv = d.
- [x] Si a et b sont premiers entre eux, alors pour tout entier k, il existe deux entiers u et v tels que au + bv = dk

> Solution n°4 *(exercice p. 20)*

- [ ] la relation de congruence dans N est une relation d'équivalence.
- [x] la relation de congruence dans Z est une relation d'équivalence.
- [ ] la relation de congruence dans Z est une relation d'ordre
- [ ] Aucune des assertions précédentes n'est vraie

> Solution n°5 *(exercice p. 21)*

- [x] Si un entier est congru à 0 modulo 6, alors il est divisible par 6
- [ ] Si le produit de deux entiers est congru à 0 modulo 6 alors l'un des deux est multiple de 6.
- [x] Si un entier est congru à 5 modulo 6 alors toutes ses puissances paires sont congrues à 1 modulo 6.
- [x] Si deux entiers sont congrus à 4 modulo 6, alors leur somme est congrue à 2 modulo 6.
- [ ] Si deux entiers sont congrus à 4 modulo 6, alors leur produit est congru à 2 modulo 6
- [x] Si un entier est congru à 4 modulo 6 alors toutes ses puissances sont aussi congrues à 4 modulo 6.

> Solution n°6 *(exercice p. 24)*

- ( ) x ≡ 17 [19].
- (•) x ≡ 13 [19].
- ( ) x ≡ 1 [19].
- ( ) x ≡ 15 [19].

Notons a l'inconnue auxiliaire a = cl(x) et remarquons que
cl(0)*17* cl(3). Il suffit donc de résoudre a*17* = cl(3) dans (Z/19Z) \ {cl(0)}.

Mais, si a 6= cl(0), alors a*17* = cl(3) si et seulement si a*18* = cl(3)a. Maintenant, pour tout a dans le groupe multiplicatif (Z/19Z) \ {cl(0)}, on sait que l'ordre de a, qui est le nombre d'éléments du groupe <a>, divise le nombre d'éléments de (Z/19Z) \ {cl(0)}, c'est-à-dire 18.

Ainsi, pour tout élément a de (Z/19Z) \ {cl(0)}, a*18* = cl(1). L'équation étudiée se simplifie donc grandement en cl(1) = cl(3)a, c'est-à-dire a = (cl(3))−1. Sa résolution se ramène donc à la recherche de l'inverse de cl(3) dans Z/19Z ; on écrit alors une relation de Bézout : 13 × 3 − 2 × 19 = 1 et on en déduit que (cl(3))−1 = cl(13).

Finalement les solutions de l'équation initiale sont donc
x ≡ 13 [19].

> Solution n°7 *(exercice p. 24)*

☐	1
☑	2
☐	4
☐	Une infinité

Références

Bibliographie

[1] F. Liret, D. Martinais, Algèbre Licence 1ère année MIAS-MASS-SM, éditions Dunod, 2002

[2] François Liret, Maths en pratique à l'usage des étudiants Cours et exercices, éditions Dunod, 2006

[3] Jean Romain Heu Cours d'Algèbre générale 2016

[4] Claude Deschamps, André Warufsel, Mathématiques tout en un 1ière année, MPSI, PCSI, , éditions Dunod, 2003