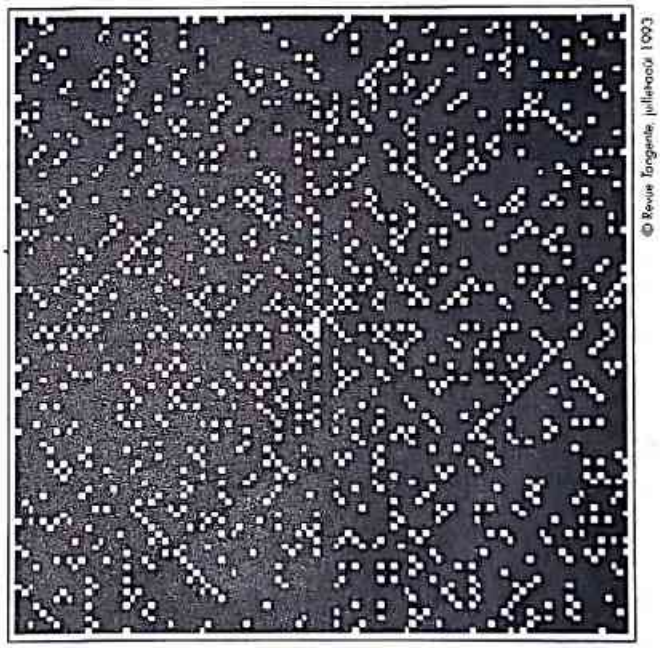
1 Arithmétique

Introduction

L'arithmétique est un des secteurs scientifiques les plus anciens et les plus féconds. Fondée essentiellement par les pythagoriciens pour qui tout était nombre, elle a connu de grands progrès sous l'impulsion de Fermat, Euler, Lagrange, Gauss et Legendre.

Longtemps considérée comme la branche la plus abstraite et la moins utile des mathématiques, elle connaît aujourd'hui de nombreuses applications en informatique, en électronique et en cryptographie.



La spirale d'Ulam (voir p. 25).

SOMMAIRE

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

1.1. L'ensemble $\mathbb{N}$

$\mathbb{N}$ désigne l'ensemble des entiers naturels et $\mathbb{N}^*$ l'ensemble des entiers naturels non nuls.

On a : $\mathbb{N} = \{0 ; 1 ; 2 ; 3 ; \ldots ; n ; n+1 ; \ldots\}$ et $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Addition et multiplication dans $\mathbb{N}$

$\mathbb{N}$ est muni de deux opérations :

- l'addition, notée + ;
- la multiplication, notée ×.

Pour tous entiers naturels a et b, $a + b$ et $a \times b$ sont des entiers naturels ; on dit que l'addition et la multiplication dans $\mathbb{N}$ sont des ***lois de composition internes***.

Les propriétés de l'addition et de la multiplication dans $\mathbb{N}$ sont résumées dans le tableau ci-contre où a, b et c désignent des entiers naturels.

Addition dans $\mathbb{N}$	Multiplication dans $\mathbb{N}$
$a + 0 = 0 + a = a$ *0 est élément neutre pour +*	$a \times 1 = 1 \times a = a$ *1 est élément neutre pour ×*
$a + (b + c) = (a + b) + c$ *+ est associative*	$a \times (b \times c) = (a \times b) \times c$ *× est associative*
$a + b = b + a$ *+ est commutative*	$a \times b = b \times a$ *× est commutative*
$a \times (b + c) = a \times b + a \times c$ *× est distributive par rapport à +*	
$a + c = b + c \Rightarrow a = b$ $(c \in \mathbb{N})$	$a \times c = b \times c \Rightarrow a = b$ $(c \in \mathbb{N}^*)$
$a + b = 0 \Rightarrow a = b = 0$	$a \times b = 1 \Rightarrow a = b = 1$

Remarque

Lorsqu'il n'y a pas d'ambiguïté le produit $a \times b$ est noté : ab.

Ordre dans $\mathbb{N}$

On définit dans $\mathbb{N}$ une relation, notée $\leq$, par : $\forall (a ; b) \in \mathbb{N}^2, (a \leq b \Leftrightarrow \exists c \in \mathbb{N}, b = a + c)$.

Cette relation possède les propriétés suivantes, dont la démonstration est immédiate.

Propriétés 1

Pour tous entiers naturels a, b et c, on a :

- $a \leq a$ ***(la relation $\leq$ est réflexive)***
- **si $a \leq b$ et $b \leq a$, alors $a = b$** ***(la relation $\leq$ est antisymétrique)***
- **si $a \leq b$ et $b \leq c$, alors $a \leq c$** ***(la relation $\leq$ est transitive).***

*On dit que $\leq$ dans $\mathbb{N}$ est une **relation d'ordre**.*

Remarque

*Deux entiers naturels a et b sont toujours comparables, c'est-à-dire on a toujours : $a \leq b$ ou $b \leq a$; on dit que $\leq$ dans $\mathbb{N}$ est une relation **d'ordre total**.*

Nous admettons la propriété suivante.

Propriété 2

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Exemples

- Le plus petit élément de $\mathbb{N}$ est 0.
- Le plus petit élément de l'ensemble $\{2n + 7, n \in \mathbb{N}\}$ est 7.

Raisonnement par récurrence

Considérons les premiers entiers naturels non nuls et comparons la somme de leurs cubes au carré de leur somme.

On a : $1^3 = 1$ et $1^2 = 1$

$1^3 + 2^3 = 9$ et $(1 + 2)^2 = 9$

$1^3 + 2^3 + 3^3 = 36$ et $(1 + 2 + 3)^2 = 36$

$1^3 + 2^3 + 3^3 + 4^3 = 100$ et $(1 + 2 + 3 + 4)^2 = 100$.

Ces observations conduisent à conjecturer que : $\forall\, n \in \mathbb{N}^*,\ 1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$.
Étant dans l'impossibilité d'effectuer une infinité de vérifications, nous allons utiliser un raisonnement par récurrence, dont le principe peut être illustré par la situation suivante : « *si, dans une rangée de voitures, la première est verte et derrière toute voiture verte il y a une voiture verte, alors toutes les voitures sont vertes* ».

L

Pour démontrer qu'une proposition P(n), qui concerne un entier naturel n, est vraie pout tout n supérieur ou égal à n_0, on procède en deux étapes :

- **on démontre que : P(n_0) est vraie ;**
- **on démontre que : pour tout entier k supérieur ou égal à n_0, si P(k) est vraie alors P($k + 1$) est vraie.**

Exemples

• Soit P(n) la proposition : « $1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$ ».
– Nous avons déjà vérifié que : P(1) est vraie.
– Soit k un entier naturel supérieur ou égal à 1.
Si P(k) est vraie, on a : $1^3 + 2^3 + \ldots + k^3 = (1 + 2 + \ldots + k)^2$;
donc :

$$\begin{aligned} 1^3 + 2^3 + \ldots + k^3 + (k+1)^3 &= (1 + 2 + \ldots + k)^2 + k(k+1)^2 + (k+1)^2 \\ &= \left[\frac{k(k+1)}{2}\right]^2 + 2\,\frac{k(k+1)}{2}(k+1) + (k+1)^2 \\ &= \left[\frac{k(k+1)}{2} + (k+1)\right]^2 \\ &= [1 + 2 + \ldots + k + (k+1)]^2 ; \end{aligned}$$

c'est-à-dire : P($k + 1$) est vraie.
On en déduit que, pour tout entier naturel n non nul, P(n) est vraie.

• Démontrons que pour tout entier naturel n supérieur ou égal à 4, on a : $n^2 \leq 2^n$.
Soit Q(n) la proposition : « $n^2 \leq 2^n$ ».
– On a : $4^2 \leq 2^4$; donc : Q(4) est vraie.
– Soit k un entier naturel supérieur ou égal à 4.
Si Q(k) est vraie, on a : $k^2 \leq 2^k$.
Or : $\frac{k+1}{k} = 1 + \frac{1}{k}$; donc : $\frac{k+1}{k} \leq \frac{5}{4}$ et $(k+1)^2 \leq 2k^2$.
Donc : $(k+1)^2 \leq 2^{k+1}$; c'est-à-dire : Q($k + 1$) est vraie.

On en déduit que, pour tout entier naturel n supérieur ou égal à 4, Q(n) est vraie.

1.2. L'ensemble $\mathbb{Z}$

$\mathbb{Z}$ désigne l'ensemble des entiers relatifs et $\mathbb{Z}^*$ l'ensemble des entiers relatifs non nuls.
On a : $\mathbb{Z} = \{\ldots ; n-1 ; n ; \ldots ; -2 ; -1 ; 0 ; 1 ; 2 ; \ldots\}$ et $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

Addition dans $\mathbb{Z}$

L'addition dans $\mathbb{Z}$ possède les propriétés suivantes.

Propriétés 1

Pour tous entiers relatifs a, b et c, on a :

(1)	$a + b \in \mathbb{Z}$	***(+ dans $\mathbb{Z}$ est une loi de composition interne)***
(2)	$a + (b + c) = (a + b) + c$	***(+ est associative)***
(3)	$a + 0 = 0 + a = a$	***(0 est élément neutre pour +)***
(4)	$\exists\, a' \in \mathbb{Z},\ a + a' = a' + a = 0$	***(tout élément de $\mathbb{Z}$ a un opposé dans $\mathbb{Z}$)***
(5)	$a + b = b + a$	***(+ est commutative).***

Notation et vocabulaire

- L'opposé d'un entier relatif a est unique ; on le note $-a$ et on l'appelle ***symétrique*** de a pour $+$.
- Pour résumer les 4 premières propriétés, on dit que $(\mathbb{Z}, +)$ est un ***groupe*** ;
  pour résumer les 5 propriétés, on dit que $(\mathbb{Z}, +)$ est un groupe ***commutatif***.
- Plus généralement, un ensemble muni d'une loi de composition interne est un groupe lorsque :
  - la loi est associative ;
  - l'ensemble possède un élément neutre pour cette loi ;
  - tout élément de l'ensemble admet un symétrique pour cette loi dans cet ensemble.

Ce groupe est commutatif si de plus la loi est commutative.

Exemples

- $(\mathbb{R}, +)$ est un groupe commutatif.
  $(\mathbb{N}, +)$ n'est pas un groupe.
- Soit $\mathcal{I}$ l'ensemble des isométries du plan.

$(\mathcal{I}, \circ)$ est un groupe ; en effet :
- la composée de deux isométries est une isométrie ;
- la composée des isométries est associative ;
- l'application identique, qui est une isométrie, est élément neutre pour $\circ$;
- le symétrique d'une isométrie pour $\circ$ est son isométrie réciproque.

Le groupe $(\mathcal{I}, \circ)$ n'est pas commutatif.

Propriété 2

Pour tous entiers relatifs a, b et c, on a : $a + c = b + c \Rightarrow a = b$.

En effet, si $a + c = b + c$, alors : $a + c + (-c) = b + c + (-c)$; donc : $a = b$.

Multiplication dans $\mathbb{Z}$

La multiplication dans $\mathbb{Z}$ possède les propriétés suivantes.

Propriétés 1

Pour tous entiers relatifs a, b et c, on a :

(1')	$a \times b \in \mathbb{Z}$	***($\times$ dans $\mathbb{Z}$ est une loi de composition interne)***
(2')	$a \times (b \times c) = (a \times b) \times c$	***($\times$ est associative)***
(3')	$a \times (b + c) = a \times b + a \times c$	***($\times$ est distributive par rapport à $+$)***
(4')	$a \times b = b \times a$	***($\times$ est commutative)***
(5')	$a \times 1 = 1 \times a = a$	***(1 est élément neutre pour $\times$).***

Vocabulaire

Pour résumer les propriétés (1), (2), (3), (4), (5) de l'addition et les propriétés (1'), (2'), (3'), (4'), (5') de la multiplication, on dit que $(\mathbb{Z}, +, \times)$ est un ***anneau commutatif unitaire***.

Propriétés 2

Pour tous entiers relatifs a, b et c ($c \neq 0$), on a :

- $a \times 0 = 0$;
- $ca = cb \Rightarrow a = b$.

Démonstration

Nous ne démontrerons que la première propriété.

On a : $aa + a \times 0 = a(a + 0) = aa = aa + 0$; donc : $a \times 0 = 0$.

Ordre dans $\mathbb{Z}$

Pour tous nombres entiers relatifs a et b, on pose : $b - a = b + (-a)$.

On définit dans $\mathbb{Z}$ une relation, notée $\leq$, par : $\forall (a ; b) \in \mathbb{Z}^2$, $(a \leq b \Leftrightarrow b - a \in \mathbb{N})$.

Cette relation est une relation d'ordre total.

Nous admettons les propriétés 1 et 2 suivantes.

Propriétés 1

Soit a et b deux entiers relatifs.
- **Pour tout entier relatif c, on a :** $a \leq b \Leftrightarrow a + c \leq b + c$.
- **Pour tout entier c strictement positif, on a :** $a \leq b \Leftrightarrow a \times c \leq b \times c$.
- **Pour tout entier c strictement négatif, on a :** $a \leq b \Leftrightarrow a \times c \geq b \times c$.

Propriétés 2

- **Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.**
- **Toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.**

Exemple

L'ensemble $\{n \in \mathbb{Z}, (n+2)^2 \leq 6\}$ est borné.
Son plus grand élément est 0 et son plus petit élément est -4.

Propriété 3

Soit a et b deux entiers relatifs tels que : $b \neq 0$.
Il existe un entier relatif n tel que : $nb \geq a$.

On dit que $\mathbb{Z}$ est archimédien.

Démonstration

1er cas : $b \geq 1$
- si $a \geq 0$, il suffit de prendre : $n = a$;
- si $a < 0$, il suffit de prendre : $n = 0$.

2e cas : $b \leq -1$
On a : $-b \geq 1$; donc il existe un entier relatif m, tel que : $m(-b) \geq a$.
Il suffit donc de prendre : $n = -m$.

Division euclidienne dans $\mathbb{Z}$

Propriété

Soit a et b deux entiers relatifs tels que : $b \neq 0$.
Il existe un unique couple $(q ; r)$ de $\mathbb{Z} \times \mathbb{N}$ tel que : $a = bq + r$ et $0 \leq r < |b|$.

Les nombres q et r s'appellent respectivement le quotient et le reste de la division euclidienne de a par b. Effectuer une division euclidienne c'est déterminer son quotient et son reste.

Démonstration

- *Existence*

Soit A l'ensemble des entiers naturels de la forme : $a - bq$ $(q \in \mathbb{Z})$.

$a + |ba|$ est élément de A ; donc A est une partie non vide de $\mathbb{N}$, qui admet un plus petit élément r.

r est élément de A ; donc $r \geq 0$ et $r = a - bq$ $(q \in \mathbb{Z})$.

De plus, $r < |b|$ (sinon, $r - |b| = a - bq - |b| = a - bq'$; donc, $r - |b|$ serait un élément de A, plus petit que r ; c'est-à-dire, r ne serait plus le plus petit élément de A).

On en déduit qu'il existe un couple $(q ; r)$ de $\mathbb{Z} \times \mathbb{N}$ tel que : $a = bq + r$ et $0 \leq r < |b|$.

- *Unicité*

Soit $(q ; r)$ et $(q' ; r')$ deux couples de $\mathbb{Z} \times \mathbb{N}$ tels que : $a = bq + r$, $a = bq' + r'$, $0 \leq r < |b|$ et $0 \leq r' < |b|$.

On a : $0 = b(q' - q) + (r' - r)$; donc : $|b|\,|q' - q| = |r' - r|$.

Or : $-|b| < r' - r < |b|$; donc : $|r' - r| < |b|$.

On en déduit que : $|q' - q| = 0$ (si $|q' - q| \geq 1$, on aurait : $|b|\,|q' - q| \geq |b|$).

De plus : $|r' - r| = |b|\,|q' - q|$; donc : $q' = q$ et $r' = r$.

Exemples

Effectuer la division euclidienne de a par b dans chacun des cas suivants :

$a = 53$ et $b = 12$; $a = -53$ et $b = 12$; $a = 53$ et $b = -12$; $a = -53$ et $b = -12$.

• On a : $53 = 12 \times 4 + 5$ et $0 \leq 5 < 12$.
Donc : 4 et 5 sont respectivement le quotient et le reste de la division euclidienne de 53 par 12.

• On a : $-53 = 12 \times (-4) - 5$
$= 12 \times (-5) + 7$ et $0 \leq 7 < 12$.
Donc : – 5 et 7 sont respectivement le quotient et le reste de la division euclidienne de – 53 par 12.

• On a : $53 = (-12) \times (-4) + 5$ et $0 \leq 5 < 12$.
Donc : – 4 et 5 sont respectivement le quotient et le reste de la division euclidienne de 53 par – 12.

• On a : $-53 = (-12) \times 4 - 5$
$= (-12) \times 5 + 7$ et $0 \leq 7 < 12$.
Donc : 5 et 7 sont respectivement le quotient et le reste de la division euclidienne de – 53 par – 12.

1.3. Numération

Bases de numération

Toutes les civilisations anciennes de Chine, Mésopotamie, Égypte, Amérique du Sud ... ont inventé un système de numération. Mais ces différents systèmes ne permettaient pas d'effectuer facilement les opérations.

Le système décimal (base dix) a l'avantage de rendre simples toutes les opérations, grâce à l'invention du 0 et à la valeur de position des chiffres.

Le système binaire (base deux) est adapté à l'informatique qui utilise également le système hexadécimal (base seize) pour réduire la taille de l'écriture des nombres (code ASC II).

Nous admettons la propriété suivante.

Propriété

Soit b un entier naturel supérieur ou égal à 2.
Tout entier naturel x non nul peut s'écrire de façon unique $\sum_{k=0}^{p} a_k b^k$, où les a_k sont des entiers naturels tels que : $0 \leq a_k < b$ et $a_p \neq 0$.

On écrit : $x = \overline{a_p a_{p-1} \ldots a_2 a_1 a_0}^{b}$. Cette écriture est appelée ***écriture de x en base b.***

Par convention, les écritures sans « barre » sont en base 10.

Remarques

Soit $x = \overline{a_p a_{p-1} \ldots a_2 a_1 a_0}^{b} = a_p b^p + a_{p-1} b^{p-1} + \ldots + a_2 b^2 + a_1 b + a_0$.

• *On a : $x = b(a_p b^{p-1} + a_{p-1} b^{p-2} + \ldots + a_2 b + a_1) + a_0$, avec $0 \leq a_0 < b$;*

donc $q_0 = \overline{a_p a_{p-1} \ldots a_2 a_1}^{b}$ et a_0 sont respectivement le quotient et le reste de la division euclidienne de x par b.

• *On a : $q_0 = b(a_p b^{p-2} + a_{p-1} b^{p-3} + \ldots + a_2) + a_1$, avec $0 \leq a_1 < b$;*

donc $q_1 = \overline{a_p a_{p-1} \ldots a_2}^{b}$ et a_1 sont respectivement le quotient et le reste de la division euclidienne de q_0 par b.
On peut ainsi déterminer de proche en proche l'écriture de x en base b.

Exemples

• Écrire dans le système décimal le nombre : $\overline{423}^{5}$.

On a : $\overline{423}^{5} = 4 \times 5^2 + 2 \times 5^1 + 3 \times 5^0$
$= 4 \times 25 + 2 \times 5 + 3$
$= 113$.

• Écrire le nombre 127 en base sept.
On effectue les divisions successives par 7, comme indiqué sur le schéma ci-contre.
On en déduit que : $127 = \overline{241}^{7}$.

127	7
1	18 | 7
	4 | 2

Système binaire

Pour écrire un nombre en base deux, l'ensemble des chiffres utilisés est : {0 ; 1}.

Exemples

• Écrire dans le système décimal le nombre : $\overline{10100111001}^2$.

On a : $\overline{10100111001}^2 = 2^{10} + 2^8 + 2^5 + 2^4 + 2^3 + 2^0$
$= 1\,024 + 256 + 32 + 16 + 8 + 1$
$= 1\,337.$

• Écrire le nombre 87 en base deux.

On effectue les divisions successives par 2, comme indiqué sur le schéma ci-contre.

On en déduit que : $87 = \overline{1010111}^2$.

87	2
1	43 | 2
	1 | 21 | 2
	1 | 10 | 2
	0 | 5 | 2
	1 | 2 | 2
	0 | 1

Système hexadécimal

Pour écrire un nombre en base seize, l'ensemble des chiffres utilisés est :
{0 ; 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 ; 9 ; A ; B ; C ; D ; E ; F}.
(A, B, C, D, E et F représentent respectivement 10, 11, 12, 13, 14 et 15.)

Exemples

• Écrire dans le système décimal le nombre : $\overline{F0A5}^{16}$.

On a : $\overline{F0A5}^{16} = 15 \times 16^3 + 0 \times 16^2 + 10 \times 16^1 + 5 \times 16^0$
$= 61\,440 + 160 + 5$
$= 61\,605.$

• Écrire le nombre 64 206 en base seize.

On effectue les divisions successives par 16, comme indiqué sur le schéma ci-contre.

On en déduit que : $64\,206 = \overline{FACE}^{16}$.

64 206	16
14	4 012 | 16
	12 | 250 | 16
	10 | 15

1.4. Travaux dirigés

Un damier comporte 1 024 cases sur 1 024 toutes blanches sauf une, peinte en noir, à un endroit non précisé du damier. On dispose, en nombre suffisant, de « triminos » en forme de « L ». Est-il possible, à l'aide des triminos, de paver toutes les cases blanches du damier, sans déborder et sans que deux triminos ne se chevauchent ?

Un trimino, comme son nom l'indique, recouvre trois cases du damier.

Solution

On remarque que $1\,024 = 2^{10}$.
Soit P(n) la proposition : « un damier de côté 2^n, privé d'une case, peut être pavé par des triminos ».

• Pour $n = 1$, un damier 2×2 privé d'une case est un trimino. Donc P(1) est vraie.

• Soit k un entier naturel supérieur ou égal à 1.

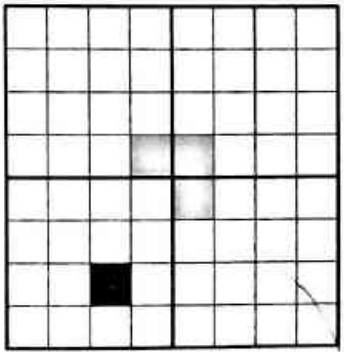
Supposons P(k) vraie et considérons un damier de côté 2^{k+1}, privé d'une case.

Ce damier peut être partagé en quatre « sous-damiers » de côté 2^k. L'un de ces quatre sous-damiers contient la case noire ; on peut donc le paver de triminos.

Posons au centre un trimino à cheval sur les trois autres. Chacun des sous-damiers restants, privé de la case couverte par le trimino, peut être à son tour pavé par des triminos.

Donc P($k + 1$) est vraie.

On en déduit que le damier de $1\,024 \times 1\,024$ cases privé d'une case peut être pavé par des triminos.



Exercices

1.a Résoudre dans $\mathbb{N}^2$ le système : $\begin{cases} xy \leq 2x \\ x + y = 4 \end{cases}$.

1.b Résoudre dans $\mathbb{Z}^2$ le système : $\begin{cases} xy = 1 \\ 3x + y = -4 \end{cases}$.

1.c Démontrer par récurrence que pour tout entier naturel non nul n, on a :

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

1.d Démontrer par récurrence que pour tout entier naturel non nul n, on a : $n! \geq 2^{n-1}$.

1.e Effectuer la division euclidienne de a par b dans chacun des cas suivants.

- $a = 59$ et $b = 18$
- $a = -59$ et $b = 18$
- $a = 59$ et $b = -18$
- $a = -59$ et $b = -18$
- $a = 6\,941$ et $b = 358$
- $a = 358$ et $b = 6\,941$.

1.f Déterminer l'entier naturel qui, divisé par 23, a pour reste 1 et qui, divisé par 17, a le même quotient et pour reste 13.

1.g Écrire en base deux chacun des nombres suivants : 9 ; 17 ; 205 ; 864.

1.h Écrire en base dix chacun des nombres suivants : $\overline{1011}^2$; $\overline{1101101}^2$.

2 Divisibilité dans $\mathbb{Z}$

2.1. Multiples et diviseurs d'un entier relatif

Définition et propriétés

Définition

Soit a et b deux entiers relatifs.
On dit que a est un multiple de b s'il existe un entier relatif k tel que : $a = kb$.
Si de plus $b \neq 0$, on dit que b est un diviseur de a ou que b divise a.

Exemples

- On a : $143 = 11 \times 13$; donc : 143 est multiple de 11 et de 13 ; 13 et 11 divisent 143.
- On a : $12 = (-4) \times (-3)$; donc : 12 est multiple de -4 ; -4 divise 12.

Remarques

- *Tout entier relatif est multiple de 1 et -1.*
1 et -1 divisent tout entier relatif.
- *0 est multiple de tout entier relatif.*
Tout entier relatif non nul divise 0, mais 0 ne divise aucun entier relatif.
- *Lorsque $b \neq 0$, a est multiple de b (ou b divise a) si et seulement si le reste de la division euclidienne de a par b est nul.*

Les propriétés suivantes sont présentées en termes de diviseurs. Nous laissons au lecteur le soin de les énoncer en termes de multiples. Selon le contexte, l'une ou l'autre de ces deux formes pourra être utilisée.

Propriété 1

Soit a et b deux entiers relatifs non nuls.
Si b divise a, alors : $|b| \leq |a|$.

Démonstration

Si b divise a, alors il existe un entier relatif non nul q tel que : $a = bq$.
On a : $1 \leq |q|$; donc : $|b| \leq |b||q|$.
C'est-à-dire : $|b| \leq |a|$.

Propriétés 2

Soit a, b et c trois entiers relatifs ($a \neq 0$, $b \neq 0$).
(1) a divise a.
(2) Si a divise b et b divise a, alors $a = b$ ou $a = -b$.
(3) Si a divise b et b divise c, alors a divise c.

Démonstration

(1) et (3) découlent immédiatement de la définition de la divisibilité.
(2) D'après la propriété 1, a divise $b \Rightarrow |a| \leq |b|$ et b divise $a \Rightarrow |b| \leq |a|$;
donc : (a divise b et b divise a) $\Rightarrow |a| = |b|$.

Propriété 3

Soit a, b et c trois entiers relatifs ($a \neq 0$).
Si a divise b et c, alors pour tous entiers relatifs p et q, a divise $pb + qc$.

On dit encore que a divise toute combinaison linéaire de b et c dans $\mathbb{Z}$.
Cette propriété découle immédiatement de la définition de la divisibilité.

Exemples

- La somme ou la différence de deux entiers relatifs pairs est un entier relatif pair.
- Le produit d'un entier relatif par un entier relatif pair est un entier relatif pair.

Ensemble des multiples d'un entier relatif

Soit b un entier relatif.
Les multiples de b sont les nombres : ..., $b \times (-2)$, $b \times (-1)$, $b \times 0$, $b \times 1$, $b \times 2$, ...
Ces nombres sont de la forme : bk, où $k \in \mathbb{Z}$.

Notation

L'ensemble des multiples de b ($b \in \mathbb{Z}$) est noté $b\mathbb{Z}$.

Exemples

- $3\mathbb{Z} = \{... ; -9 ; -6 ; -3 ; 0 ; 3 ; 6 ; 9 ; ...\}$
- $-2\mathbb{Z} = \{... ; -6 ; -4 ; -2 ; 0 ; 2 ; 4 ; 6 ; ...\}$
- $1\mathbb{Z} = \mathbb{Z}$
- $0\mathbb{Z} = \{0\}$.

Remarque

Pour tout entier relatif b, $(b\mathbb{Z}, +)$ est un groupe commutatif.

Ensemble des diviseurs d'un entier relatif

Notation

Soit a un entier relatif.
On note : $\mathcal{D}(a)$ l'ensemble des diviseurs de a.

Exemples

- $\mathcal{D}(4) = \{-4 ; -2 ; -1 ; 1 ; 2 ; 4\}$
- $\mathcal{D}(-6) = \{-6 ; -3 ; -2 ; -1 ; 1 ; 2 ; 3 ; 6\}$
- $\mathcal{D}(1) = \{-1 ; 1\}$
- $\mathcal{D}(0) = \mathbb{Z}^*$.

Remarque

Pour tout entier relatif a non nul, $\mathcal{D}(a)$ est un ensemble fini non vide.

2.2. Congruence modulo n ($n \in \mathbb{N}^*$)

Définition et propriétés immédiates

Définition

Soit n un entier naturel non nul, a et b deux entiers relatifs.
On dit que a est congru à b modulo n si $a - b$ est un multiple de n.

On écrit : $a \equiv b\ [n]$.

Exemples

• $54 \equiv 4\ [10]$; • $-81 \equiv 0\ [9]$; • $9 \equiv -1\ [10]$; • $-5 \equiv 2\ [7]$.

Remarques

• $a \equiv 0\ [n] \Leftrightarrow a$ *multiple de* n ;
• $a \equiv b\ [n] \Leftrightarrow a - b$ *multiple de* n ;
• *si* r *désigne le reste de la division euclidienne de* a *par* n, *alors* : $a \equiv r\ [n]$.

Les propriétés suivantes sont des conséquences immédiates de la définition.

Propriétés

Soit n un entier naturel non nul, a, b et c trois entiers relatifs.
• $a \equiv a\ [n]$ *(la relation de congruence modulo n est réflexive)*
• **Si** $a \equiv b\ [n]$, **alors** $b \equiv a\ [n]$ *(la relation de congruence modulo n est symétrique)*
• **Si** $a \equiv b\ [n]$ **et** $b \equiv c\ [n]$, **alors** $a \equiv c\ [n]$ *(la relation de congruence modulo n est transitive).*

Autres propriétés

Propriété 1

Soit n un entier naturel non nul, a et a' deux entiers relatifs, r et r' les restes respectifs des divisions euclidiennes de a et a' par n.
On a : $a \equiv a'\ [n] \Leftrightarrow r = r'$.

Démonstration

Désignons par q et q' les quotients respectifs des divisions euclidiennes de a et a' par n.
On sait que : $a = nq + r$ et $0 \leq r < n$; $a' = nq' + r'$ et $0 \leq r' < n$.
Donc : $a - a' = (b - b')n + r - r'$, avec $-n < r - r' < n$.
On en déduit que : $a \equiv a'\ [n] \Leftrightarrow a - a'$ multiple de n
$\Leftrightarrow r - r'$ multiple de n
$\Leftrightarrow r - r' = 0$.

Propriétés 2

Soit n un entier naturel non nul et a, a', b, b' quatre entiers relatifs.
• **Si** $a \equiv a'\ [n]$ **et** $b \equiv b'\ [n]$, **alors** $a + b \equiv a' + b'\ [n]$.
• **Si** $a \equiv a'\ [n]$ **et** $b \equiv b'\ [n]$, **alors** $a \times b \equiv a' \times b'\ [n]$.

On dit que la congruence modulo n est compatible avec l'addition et la multiplication dans $\mathbb{Z}$.

Démonstration

• On a : $(a' + b') - (a + b) = (a' - a) + (b' - b)$;
donc : $(a' - a \in n\mathbb{Z}$ et $b' - b \in n\mathbb{Z}) \Rightarrow (a' + b') - (a + b) \in n\mathbb{Z}$.
• On a : $(a' \times b') - (a \times b) = b'(a' - a) + a(b' - b)$;
donc : $(a' - a \in n\mathbb{Z}$ et $b' - b \in n\mathbb{Z}) \Rightarrow (a' \times b') - (a \times b) \in n\mathbb{Z}$.

Remarque

Si k est un entier naturel non nul, on a : $a \equiv a'$ [n] $\Rightarrow$ $a^k \equiv a'^k$ [n].

Exemples

On considère les nombres a et b tels que : $a = 137$ et $b = 73$.
Déterminer les restes des divisions euclidiennes de $a + b$, ab, $3a - 2b$ et $a^2 + 3b^3$ par 25.
On a : $a \equiv 12$ [25] et $b \equiv -2$ [25].

- On a : $a + b \equiv 10$ [25].
  Or : $0 \leq 10 < 25$; donc 10 est le reste de la division euclidienne de $a + b$ par 25.
- On a : $ab \equiv -24$ [25] ; donc : $ab \equiv 1$ [25].
  Or : $0 \leq 1 < 25$; donc 1 est le reste de la division euclidienne de ab par 25.
- On a : $3a - 2b \equiv 40$ [25] ; donc : $3a - 2b \equiv 15$ [25].
  Or : $0 \leq 15 < 25$; donc 15 est le reste de la division euclidienne de $3a - 2b$ par 25.
- On a : $a^2 + 3b^3 \equiv 120$ [25] ; donc : $a^2 + 3b^3 \equiv 20$ [25].
  Or : $0 \leq 20 < 25$; donc 20 est le reste de la division de $a^2 + 3b^3$ par 25.

2.3. Utilisations des congruences

Déterminations de restes

1. Déterminer le reste de la division euclidienne de $7^{2\,002}$ par 9.
On a : $7^0 \equiv 1$ [9] ; $7^1 \equiv 7$ [9] ; $7^2 \equiv 4$ [9] ; $7^3 \equiv 1$ [9].
$2\,002 = 3 \times 667 + 1$.
Donc : $(7^3)^{667} \times 7 \equiv 1^{667} \times 7$ [9] ; c'est-à-dire : $7^{2\,002} \equiv 7$ [9].
Or : $0 \leq 7 < 9$; donc 7 est le reste de la division euclidienne de $7^{2\,002}$ par 9.

2. Déterminer, suivant les valeurs de l'entier naturel n, le reste de la division euclidienne de 5^n par 3.
On a : $5^0 \equiv 1$ [3] ; $5^1 \equiv 2$ [3] ; $5^2 \equiv 1$ [3].

- Si $n = 2k$ ($k \in \mathbb{N}$), on a : $(5^2)^k \equiv 1^k$ [3] ; donc : $5^n \equiv 1$ [3].
- Si $n = 2k + 1$ ($k \in \mathbb{N}$), on a : $(5^2)^k \times 5 \equiv 1^k \times 5$ [3] ; donc : $5^n \equiv 2$ [3].

Démonstrations de propriétés

1. **Soit n un entier naturel. Démontrer que $n(n^4 - 1)$ est multiple de 5.**
On distingue cinq cas : $n \equiv 0$ [5], $n \equiv 1$ [5], ... , $n \equiv 4$ [5].
Les résultats sont regroupés dans le tableau de congruences ci-contre.
On en déduit que $n(n^4 - 1)$ est multiple de 5.

n	0	1	2	3	4
$n^4 - 1$	4	0	0	0	0
$n(n^4 - 1)$	0	0	0	0	0

2. **Soit n un entier naturel.**
1°) Démontrer que le reste de la division euclidienne de n^2 par 8 est 0, 1 ou 4.
2°) En déduire que les nombres de la forme $8k + 7$ ($k \in \mathbb{Z}$) ne sont pas la somme de trois carrés parfaits.

1°) On distingue huit cas : $n \equiv 0$ [8], $n \equiv 1$ [8], ... , $n \equiv 7$ [8].
Les résultats sont regroupés dans le tableau de congruences ci-contre.
On en déduit que le reste de la division euclidienne de n^2 par 8 est 0, 1 ou 4.

n	0	1	2	3	4	5	6	7
n^2	0	1	4	1	0	1	4	1

2°) L'ensemble des restes possibles de la division euclidienne par 8 de la somme de trois carrés parfaits est le même que l'ensemble des restes possibles de la division euclidienne par 8 de la somme de trois éléments de {0 ; 1 ; 4}.

Le tableau ci-dessous regroupe les restes possibles :

(a, b, c)	(0, 0, 0)	(0, 0, 1)	(0, 0, 4)	(0, 1, 1)	(0, 1, 4)	(0, 4, 4)	(1, 1, 1)	(1, 1, 4)	(1, 4, 4)	(4, 4, 4)
reste	0	1	4	2	5	0	3	6	1	4

On en déduit que les nombres de la forme $8k + 7$ ($k \in \mathbb{Z}$) ne sont pas la somme de trois carrés parfaits.

Congruences particulières

Les critères de divisibilité par 2, 3, 4 ,5, 9 et 11 ont été utilisés au collège. Nous allons, grâce aux congruences, démontrer ces résultats et les généraliser à la détermination des restes de certaines divisions.

Dans cette partie, x désigne un entier naturel non nul et $\overline{a_p a_{p-1} \ldots a_0}$ son écriture décimale.

On a : $x = a_p 10^p + a_{p-1} 10^{p-1} + \ldots + a_1 10^1 + a_0$.

1. *Congruences modulo 5*

***a)* Démontrer que :** $x \equiv a_0$ [5].

***b)* Déterminer les restes des divisions euclidiennes par 5 de 1 826, 3 252 et 27 325.**

a) On a : $10 \equiv 0$ [5] ; donc, pour tout entier naturel k non nul : $10^k \equiv 0$ [5].

On en déduit que : $a_p 10^p + a_{p-1} 10^{p-1} + \ldots + a_1 10^1 + a_0 \equiv a_0$ [5].

b) Les restes des divisions euclidiennes par 5 de 1 826, 3 252 et 27 325 sont respectivement 1, 2 et 0.

2. *Congruences modulo 4 et modulo 25*

***a)* Démontrer que :** $x \equiv \overline{a_1 a_0}$ [4] et $x \equiv \overline{a_1 a_0}$ [25].

***b)* Déterminer les restes des divisions euclidiennes par 4 et 25 de 1 826, 3 252 et 27 325.**

a) On a : $10^2 \equiv 0$ [4] et $10^2 \equiv 0$ [25] ;
donc, pour tout entier naturel k supérieur ou égal à 2 : $10^k \equiv 0$ [4] et $10^k \equiv 0$ [25].

On en déduit que : $a_p 10^p + a_{p-1} 10^{p-1} + \ldots + a_1 10^1 + a_0 \equiv a_1 10^1 + a_0$ [4]

et : $a_p 10^p + a_{p-1} 10^{p-1} + \ldots + a_1 10^1 + a_0 \equiv a_1 10^1 + a_0$ [25].

b) Les restes des divisions euclidiennes par 4 de 1 826, 3 252 et 27 325 sont respectivement 2, 0 et 1.

Les restes des divisions euclidiennes par 25 de 1 826, 3 252 et 27 325 sont respectivement 1, 2 et 0.

3. *Congruences modulo 9 et 3*

***a)* Démontrer que :** $x \equiv \sum_{k=0}^{p} a_k$ [9] et $x \equiv \sum_{k=0}^{p} a_k$ [3].

***b)* Déterminer les restes des divisions euclidiennes par 9 et 3 de 1 826, 3 252 et 27 325.**

a) On a : $10 \equiv 1$ [9] et $10 \equiv 1$ [3] ;
donc, pour tout entier naturel k : $10^k \equiv 1$ [9] et $10^k \equiv 1$ [3].

On en déduit que : $a_p 10^p + a_{p-1} 10^{p-1} + \ldots + a_1 10^1 + a_0 \equiv \sum_{k=0}^{p} a_k$ [9]

et : $a_p 10^p + a_{p-1} 10^{p-1} + \ldots + a_1 10^1 + a_0 \equiv \sum_{k=0}^{p} a_k$ [3].

b) On a : $1\,826 \equiv 1 + 8 + 2 + 6$ [9] ; donc le reste de la division de 1 826 par 9 est 8.

De même, les restes des divisions euclidiennes par 9 de 3 252 et 27 325 sont respectivement 3 et 1.
Les restes des divisions euclidiennes par 3 de 1 826, 3 252 et 27 325 sont respectivement 2, 0 et 1.

4. *Congruences modulo 11*

***a)* Démontrer que :** $x \equiv \sum_{k=0}^{p} (-1)^k a_k$ [11].

***b)* Déterminer les restes de la division euclidienne par 11 de 1 826, 3 252 et 27 325.**

a) On a : $10 \equiv -1$ [11] ; donc, pour tout entier naturel k : $10^k \equiv (-1)^k$ [11].

On en déduit que : $a_p 10^p + a_{p-1} 10^{p-1} + \ldots + a_1 10^1 + a_0 \equiv \sum_{k=0}^{p} (-1)^k a_k$ [11].

b) On a : $1\,826 \equiv -1 + 8 - 2 + 6$ [11] ; donc le reste de la division euclidienne de 1 826 par 11 est 0.

De même, les restes des divisions euclidiennes par 11 de 3 252 et 27 325 sont respectivement 7 et 1.

Exercices

2.a Combien y a-t-il de multiples de 11 compris entre – 1 000 et 1 000 ?

2.b Déterminer l'ensemble des diviseurs de 60.

2.c Déterminer les entiers naturels n et p tels que : $n^2 - p^2 = 28$.

2.d Démontrer que : $2^{32} \equiv 1$ [5].

2.e Soit n et d deux entiers relatifs non nuls tels que d divise n.
Démontrer que pour tous entiers relatifs a et b on a : $a \equiv b$ [n] $\Rightarrow a \equiv b$ [d].

2.f Sans effectuer la division euclidienne, vérifier que 23 157 est divisible par 9.

2.g Déterminer les couples $(x ; y)$ de chiffres tels que le nombre d'écriture décimale $\overline{724xy}$ soit multiple de 9.

2.h Soit a, b et c trois entiers relatifs non nuls.
1. Démontrer que si bc divise a, alors b divise a et c divise a.
2. La réciproque est-elle vraie ?

3 PPCM et PGCD de deux entiers relatifs

3.1. PPCM de deux entiers relatifs

Soit a et b deux entiers relatifs non nuls et A l'ensemble des entiers naturels non nuls appartenant à $a\mathbb{Z} \cap b\mathbb{Z}$.
$|ab| \in$ A ; donc A, partie non vide de $\mathbb{N}$, admet un plus petit élément.

Définition

Soit a et b deux entiers relatifs non nuls.
On appelle plus petit commun multiple de a et b, et on note PPCM(a ; b), le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$.

Exemples

• On a : $12\mathbb{Z} = \{\ldots ; -24 ; -12 ; 0 ; 12 ; 24 ; 36 ; 48 ; 60 ; 72 ; 84 ; 96 ; \ldots\}$
$16\mathbb{Z} = \{\ldots ; -32 ; -16 ; 0 ; 16 ; 32 ; 48 ; 64 ; 80 ; 96 ; \ldots\}$
$12\mathbb{Z} \cap 16\mathbb{Z} = \{\ldots ; -48 ; 0 ; 48 ; 96 ; \ldots\}$.
Donc : PPCM(12 ; 16) = 48.

• Déterminer le PPCM de 5 et 7.
Les multiples strictement positifs de 7 sont dans l'ordre croissant : 7 ; 14 ; 21 ; 28 ; 35 ...
Le plus petit d'entre eux qui est multiple de 5 est 35 ; donc : PPCM(5 ; 7) = 35.

Remarques

• *Pour tous entiers relatifs non nuls a et b, on a : PPCM(a ; b) = PPCM($|a|$; $|b|$).*
Dans une recherche de PPCM, on peut donc se ramener à la recherche du PPCM de deux entiers naturels non nuls.
• *Pour tous entiers naturels non nuls a et b, on a : Max(a ; b) $\leq$ PPCM(a ; b) $\leq ab$.*
• *Pour tous entiers naturels non nuls a et b, on a : PPCM(a ; b) = $a \Leftrightarrow a \in b\mathbb{Z}$.*

Propriété 1

Soit a et b deux entiers naturels non nuls et μ leur PPCM.
On a : $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$.

Démonstration

• Soit k un élément de $\mu\mathbb{Z}$.
k est multiple de μ et μ est multiple de a et de b ; donc k est multiple de a et de b.
Tout multiple de μ est multiple de a et de b ; donc : $\mu\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$.

• Soit k un élément de $a\mathbb{Z} \cap b\mathbb{Z}$.
Désignons par q et r le quotient et le reste de la division euclidienne de k par μ ; on a : $r = k - \mu q$.
k et μ sont des multiples communs à a et b ; donc : $r \in a\mathbb{Z} \cap b\mathbb{Z}$.
De plus, μ est le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$ et $0 \leq r < \mu$; donc : $r = 0$.
On en déduit que : $k \in \mu\mathbb{Z}$.
Donc : $a\mathbb{Z} \cap b\mathbb{Z} \subset \mu\mathbb{Z}$.
• On a : $\mu\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} \subset \mu\mathbb{Z}$; donc : $\mu\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

Exemple

PPCM(12 ; 16) = 48 et $12\mathbb{Z} \cap 16\mathbb{Z} = 48\mathbb{Z}$.

Propriété 2

Soit a, b et k trois entiers naturels non nuls.
On a : PPCM(ka ; kb) = kPPCM(a ; b).

Démonstration

Posons : μ = PPCM(a ; b) et μ_1 = PPCM (ka ; kb).
• Il existe deux entiers naturels non nuls a' et b' tels que : $\mu = aa'$ et $\mu = bb'$.
On a : $k\mu = kaa'$ et $k\mu = kbb'$.
$k\mu$ est un multiple commun à ka et kb ; donc : $k\mu \geq \mu_1$.
• Il existe deux entiers naturels non nuls a'' et b'' tels que : $\mu_1 = kaa''$ et $\mu_1 = kbb''$.
On a : $aa'' = bb''$; aa'' est un multiple commun à a et b, donc : $aa'' \geq \mu$.
On en déduit que : $\mu_1 \geq k\mu$.
• On a : $k\mu \geq \mu_1$ et $\mu_1 \geq k\mu$. Donc : PPCM(ka ; kb) = kPPCM(a ; b).

Exemple

PPCM(120 ; 168) = PPCM(24 × 5 ; 24 × 7) = 24 × PPCM(5 ; 7) = 24 × 35 = 840.

3.2. PGCD de deux entiers relatifs

Définition et propriétés

Soit a et b deux entiers relatifs non nuls.
L'ensemble des diviseurs communs à a et b, noté $\mathcal{D}(a ; b)$, contient 1 et est fini. Il admet donc un plus grand élément, strictement positif.

Définition

Soit a et b deux entiers relatifs non nuls.
On appelle plus grand commun diviseur de a et b, et on note PGCD(a ; b), le plus grand élément de $\mathcal{D}(a ; b)$.

Exemples

• On a : $\mathcal{D}(24) = \{-24 ; -12 ; -8 ; -6 ; -4 ; -3 ; -2 ; -1 ; 0 ; 1 ; 2 ; 3 ; 4 ; 6 ; 8 ; 12 ; 24\}$
$\mathcal{D}(30) = \{-30 ; -15 ; -10 ; -6 ; -5 ; -3 ; -2 ; -1 ; 0 ; 1 ; 2 ; 3 ; 5 ; 6 ; 10 ; 15 ; 30\}$
$\mathcal{D}(24 ; 30) = \{-6 ; -3 ; -2 ; -1 ; 0 ; 1 ; 2 ; 3 ; 5 ; 6\}$.
Donc : PGCD(24 ; 30) = 6.
• Déterminer le PGCD de 5 et 12.
On a : $\mathcal{D}(5) = \{-5 ; -1 ; 0 ; 1 ; 5\}$ et 5 ne divise pas 12.
Donc : PGCD(5 ; 12) = 1.

Remarques

• *Pour tous entiers relatifs non nuls a et b, on a : PGCD(a ; b) = PGCD($|a|$; $|b|$).*
Dans une recherche de PGCD, on peut donc se ramener à la recherche du PGCD de deux entiers naturels non nuls.
• *Pour tous entiers naturels non nuls a et b, on a : $1 \leq PGCD(a ; b) \leq Min(a ; b)$.*
• *Pour tous entiers naturels non nuls a et b, on a : $PGCD(a ; b) = b \Leftrightarrow b \in \mathcal{D}(a)$.*

Propriété 1

Soit a et b deux entiers naturels non nuls et δ leur PGCD.
On a : $\mathcal{D}(a ; b) = \mathcal{D}(\delta)$.

Démonstration

• Soit d un élément de $\mathcal{D}(\delta)$.
d divise δ et δ divise a et b ; donc d divise a et b.
Tout diviseur de δ divise a et b ; donc : $\mathcal{D}(\delta) \subset \mathcal{D}(a ; b)$.

• Soit d un élément de $\mathcal{D}(a ; b)$.

Désignons par μ le PPCM de d et δ ; on a : $\delta \leq \mu$.
a est multiple de d et de δ, donc a est multiple de μ. De même b est multiple de μ.
μ divise a et b ; donc : $\mu \leq \delta$..
On a : PPCM(d ; δ) = δ. Donc d divise δ ; c'est-à-dire : $d \in \mathcal{D}(\delta)$.

• On en déduit que : $\mathcal{D}(a ; b) = \mathcal{D}(\delta)$.

Exemple

PGCD(24 ; 30) = 6 et $\mathcal{D}(24 ; 30) = \mathcal{D}(6)$.

Propriété 2

Soit a, b et k trois entiers naturels non nuls.
On a : PGCD(ka ; kb) = k PGCD(a ; b).

Démonstration

Posons : δ = PGCD(a ; b) et δ_1 = PGCD(ka ; kb).

• Il existe deux entiers naturels non nuls a' et b' tels que : $a = \delta a'$ et $b = \delta b'$.
On a : $ka = k\delta a'$ et $kb = k\delta b'$.
$k\delta$ divise ka et kb, donc $k\delta$ divise δ_1.
Il existe un entier naturel non nul q tel que : $\delta_1 = qk\delta$ (1).

• Il existe deux entiers naturels non nuls a'' et b'' tels que : $ka = \delta_1 a''$ et $kb = \delta_1 b''$.
On a : $a = q\delta a''$ et $b = q\delta b''$; $q\delta$ divise a et b, donc : $q\delta \leq \delta$.
On en déduit que : $q = 1$.

• En remplaçant q par 1 dans (1), on obtient : PGCD(ka ; kb) = k PGCD(a ; b).

Exemple

On a : PGCD(205 ; 492) = PGCD(41 × 5 ; 41 × 12) = 41 × PGCD(5 ; 12) = 41.

Propriété 3

Soit a et b deux entiers naturels non nuls et δ leur PGCD.
Un entier relatif m est multiple de δ si et seulement si il existe deux entiers relatifs u et v tels que : $m = au + bv$.

Il revient au même de dire que : $\delta\mathbb{Z} = \{au + bv, (u ; v) \in \mathbb{Z}^2\}$.

Démonstration

• Soit u et v deux entiers relatifs.
au et bv sont multiples de δ, donc $au + bv$ est multiple de δ.
• Considérons l'ensemble A des entiers naturels qui peuvent s'écrire sous la forme $au + bv$ ($u \in \mathbb{Z}$, $v \in \mathbb{Z}$). On a : $a = a \times 1 + b \times 0$; donc : $a \in$ A.
A est une partie non vide de $\mathbb{N}$, elle admet donc un plus petit élément p.
Il existe deux entiers relatifs u' et v' tels que : $p = au' + bv'$.
Effectuons la division euclidienne de a par p ; on obtient : $a = pq + r$, avec $0 \leq r < p$.
Donc : $r = a(1 - qu') + b(-qv')$; r est de la forme : $au + bv$.
Si r était non nul, il serait un élément de A strictement inférieur à p. Donc : $r = 0$ et p divise a.
De même p divise b ; donc p divise δ.
Or, p est multiple de δ ; donc : $p = \delta$.

• Soit m un multiple de δ.
Il existe un entier relatif k tel que : $m = k\delta$; donc : $m = a(ku') + b(kv')$.

Exemple

On a : PGCD(205 ; 492) = 41 et $82 \in 41\mathbb{Z}$;
donc il existe deux entiers relatifs u et v tels que : $82 = 205u + 492v$.
En effet : $82 = 205 \times (-2) + 492 \times 1$ ou $82 = 205 \times 10 + 492 \times (-4)$.

Algorithme d'Euclide

Propriétés 1

Soit a et b deux entiers naturels tels que $a > b > 0$ et r le reste de la division euclidienne de a par b.

• Si $r = 0$, alors $\mathcal{D}(a ; b) = \mathcal{D}(b)$ • Si $r \neq 0$, alors $\mathcal{D}(a ; b) = \mathcal{D}(b ; r)$.

Démonstration

• Si $r = 0$, alors $a = bq$ et le résultat est immédiat.

• Si $r \neq 0$, alors $a = bq + r$, avec $0 < r < b$.
– On a : a combinaison linéaire de b et r dans $\mathbb{Z}$; donc tout diviseur de b et r est un diviseur de a.
On en déduit que : $\mathcal{D}(b ; r) \subset \mathcal{D}(a ; b)$.
– De plus : $r = a - bq$; c'est-à-dire : r combinaison linéaire de a et b dans $\mathbb{Z}$.
Donc tout diviseur de a et b est un diviseur de r.
On en déduit que : $\mathcal{D}(a ; b) \subset \mathcal{D}(b ; r)$.

Propriétés 2

Soit a et b deux entiers naturels tels que $a > b > 0$ et r le reste de la division euclidienne de a par b.

• Si $r = 0$, alors PGCD$(a ; b) = b$ • Si $r \neq 0$, alors PGCD$(a ; b)$ = PGCD$(b ; r)$.

Démonstration

On utilise les propriétés précédentes.

• Si $r = 0$, les ensembles $\mathcal{D}(a ; b)$ et $\mathcal{D}(b)$ sont égaux et ont le même plus grand élément.
Donc : PGCD$(a ; b) = b$.

• Si $r \neq 0$, les ensembles $\mathcal{D}(a ; b)$ et $\mathcal{D}(b ; r)$ sont égaux et ont le même plus grand élément.
Donc : PGCD$(a ; b)$ = PGCD$(b ; r)$.

Exemple

Nous avons vu que : PGCD(492 ; 205) = 41.
– Or : $492 = 205 \times 2 + 82$; donc 82 est le reste de la division euclidienne de 492 par 205.
On obtient : PGCD(492 ; 205) = PGCD(205 ; 82).
– De même : $205 = 82 \times 2 + 41$; donc 41 est le reste de la division euclidienne de 205 par 82.
On obtient cette fois : PGCD(205 ; 82) = PGCD(82 ; 41) = 41.

On déduit de ce qui précède une nouvelle méthode de recherche du PGCD, appelée algorithme d'Euclide.

M

Pour déterminer le PGCD de deux entiers naturels a et b tels que $a > b > 0$, on peut effectuer les divisions euclidiennes successives suivantes :
• division de a par b, pour obtenir $a = b \times q_0 + r_0$ (avec $0 \leq r_0 < b$) ;
• division de b par r_0, pour obtenir $b = r_0 \times q_1 + r_1$ (avec $0 \leq r_1 < r_0 < b$) ;
• division de r_0 par r_1, pour obtenir $r_0 = r_1 \times q_2 + r_2$ (avec $0 \leq r_2 < r_1 < r_0 < b$) ;
• ...

La suite (r_n), positive et strictement décroissante, s'annule après un nombre fini de divisions euclidiennes et le dernier reste non nul obtenu est égal à PGCD$(a ; b)$.

Exemple

Déterminer le PGCD de 304 939 et 151 097.
Posons : $\delta = PGCD(304\,939 ; 151\,097)$.

- $304\,939 = 151\,097 \times 2 + 2\,745$; donc : $\delta = PGCD(151\,097 ; 2\,745)$.
- $151\,097 = 2\,745 \times 55 + 122$; donc : $\delta = PGCD(2\,745 ; 122)$.
- $2\,745 = 122 \times 22 + 61$; donc : $\delta = PGCD(122 ; 61)$.
- $122 = 61 \times 2 + 0$; donc : $\delta = 61$.

On adopte généralement la disposition pratique ci-contre.

dividende	304 939	151 097	2 745	122
diviseur	151 097	2 745	122	61
reste	2 745	122	61	0

3.3. Nombres premiers entre eux

Définition et propriétés

Définition

Soit a et b deux entiers relatifs non nuls.
On dit que a et b sont premiers entre eux si leur PGCD est égal à 1.

Les seuls diviseurs communs de a et b sont alors 1 et – 1.

Exemples

- On a : PGCD(4 ; 17) = 1 ; donc 4 et 17 sont premiers entre eux.
- 60 et 135 sont tous les deux divisibles par 3 ; donc ils ne sont pas premiers entre eux.

Remarque

Soit a et b deux entiers relatifs non nuls et d un diviseur commun à a et b.
On a : $a = da'$, $b = db'$ et $PGCD(a ; b) = d\,PGCD(a' ; b')$.
d est le PGCD de a et b si et seulement si a' et b' sont premiers entre eux.

Théorème de Bézout[1]

Soit a et b deux entiers relatifs non nuls.
a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que : $au + bv = 1$.

Ce théorème est une conséquence de la propriété 3, établie au §3.2.

Exemples

- On a : $49 \times 54 + 115 \times (-23) = 1$; donc : PGCD(49 ; 115) = 1.
- Deux entiers consécutifs non nuls n et $n + 1$ sont premiers entre eux.

En effet, on a : $n \times (-1) + (n + 1) \times 1 = 1$.

Théorème de Gauss[2]

Soit a, b et c trois entiers relatifs non nuls.
Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Démonstration

Il existe trois entiers relatifs k, u et v tels que : $bc = ka$ et $au + bv = 1$.

On a : $auc + bvc = c$; donc : $a(uc + kv) = c$.

On en déduit que a divise c.

1 *Étienne Bézout, mathématicien français – 1730 - 1783.*

2 *Carl Friedrich Gauss, mathématicien, physicien et astronome allemand – 1777 - 1855.*

Exemple

Résoudre dans $\mathbb{Z}^2$ l'équation (E) : $2x - 5y = 0$.

• Soit $(x ; y)$ une solution de (E). On a : $2x = 5y$.

2 divise $5y$ et est premier avec 5 ; donc, d'après le théorème de Gauss, 2 divise y.

Il existe un entier relatif k tel que : $y = 2k$.

On en déduit que : $x = 5k$.

• Réciproquement, pour tout entier relatif k, le couple $(5k ; 2k)$ est solution de (E).

• L'ensemble des solutions de (E) est donc : $\{(5k ; 2k), k \in \mathbb{Z}\}$.

Conséquences

Soit a, b et c trois entiers relatifs non nuls.

• Si a et b sont premiers entre eux et si a et c sont premiers entre eux, alors a et bc sont premiers entre eux.

• Si a et b divisent c et si a et b sont premiers entre eux, alors ab divise c.

• Si a et b sont premiers entre eux, alors : PPCM$(a ; b) = ab$.

Démonstration

• Il existe quatre entiers relatifs u, v, u', v' tels que : $au + bv = 1$ et $au' + cv' = 1$.

En multipliant membre à membre ces deux égalités, on obtient : $a(uau' + ucv' + bvu') + bc(vv') = 1$.

Donc a est premier avec bc.

• Il existe un entier relatif a' tel que : $c = aa'$.

b divise aa' et est premier avec a ; donc il existe un entier relatif b' tel que : $a' = bb'$.

On en déduit que : $c = abb'$; donc ab divise c.

• a et b divisent PPCM$(a ; b)$, a et b sont premiers entre eux ; donc ab divise PPCM$(a ; b)$.

ab est multiple de a et de b, donc ab est multiple de PPCM$(a ; b)$.

On en déduit que : PPCM$(a ; b) = ab$.

Propriété

Soit n un entier naturel non nul et a, b, c trois entiers relatifs ($a \neq 0$).

Si a est premier avec n et si $ab \equiv ac$ [n], alors $b \equiv c$ [n].

Démonstration

On a : $ab \equiv ac$ [n] $\Leftrightarrow$ $a(b - c) \in n\mathbb{Z}$.

n divise $a(b - c)$ et est premier avec a, donc n divise $b - c$.

On en déduit que : $b \equiv c$ [n].

Relation entre le PGCD et le PPCM de deux entiers naturels

Propriété

Soit a et b deux entiers naturels non nuls, δ leur PGCD et μ leur PPCM.

On a : $\delta\mu = ab$.

Démonstration

Les entiers relatifs a' et b' tels que $a = \delta a'$ et $b = \delta b'$ sont premiers entre eux.

Donc : PPCM$(a ; b) = \delta$PPCM$(a' ; b') = \delta a'b'$.

On en déduit que : $\delta\mu = ab$.

Exemple

Déterminer le PPCM de 304 939 et 151 097.

On a vu que : PGCD(304 939 ; 151 097) = 61 ;

donc : PPCM$(304\,939 ; 151\,097) = \dfrac{304\,939 \times 151\,097}{61} = 755\,333\,903$.

3.4. Exemples d'utilisation

Détermination des coefficients d'une égalité de Bézout

1. Démontrer, en utilisant l'algorithme d'Euclide, que 564 et 271 sont premiers entre eux.
2. En déduire deux entiers relatifs u et v tels que : $564u + 271v = 1$.

Solution

1. On a : $564 = 271 \times 2 + 22$; donc : PGCD(564 ; 271) = PGCD(271 ; 22).
On a : $271 = 22 \times 12 + 7$; donc : PGCD(271 ; 22) = PGCD(22 ; 7).
On a : $22 = 7 \times 3 + 1$; donc : PGCD(22 ; 7) = PGCD(7 ; 1) = 1.
Les nombres 564 et 271 sont premiers entre eux.
2. Utilisons les divisions euclidiennes précédentes, de la dernière à la première.
On a : $1 = 22 + 7 \times (-3)$
$= 22 + (271 - 22 \times 12) \times (-3)$
$= 271 \times (-3) + 22 \times 37$
$= 271 \times (-3) + (564 - 271 \times 2) \times 37$
$= 564 \times 37 + 271 \times (-77)$.
On peut donc prendre : $(u ; v) = (37 ; -77)$.

Équations du type $ax + by = c$

D'après la propriété 3 §3.2, une équation d'inconnue $(x ; y)$ dans $\mathbb{Z}^2$ du type $ax + by = c$, a des solutions si et seulement si c est multiple du PGCD de a et b.
On se propose de résoudre dans $\mathbb{Z}^2$ l'équation (E) : $34x - 15y = 2$.
1. Résoudre dans $\mathbb{Z}^2$ l'équation (E') : $34x - 15y = 0$.
2. Déterminer une solution $(x_0 ; y_0)$ de (E).
3. Résoudre (E).

Solution

1. Soit $(x ; y)$ une solution de (E'). On a : $34x = 15y$.
15 divise $34x$ et est premier avec 34 ; donc, d'après le théorème de Gauss, 15 divise x.
Il existe un entier relatif k tel que : $x = 15k$.
On en déduit que : $y = 34k$.
Réciproquement, pour tout entier relatif k, le couple $(15k ; 34k)$ est solution de (E').
L'ensemble des solutions de (E') est donc : $\{(15k ; 34k), k \in \mathbb{Z}\}$.
2. On remarque que : $4 \times 34 = 136$ et $9 \times 15 = 135$; donc : $34 \times 8 - 15 \times 18 = 2$.
On peut prendre : $(x_0 ; y_0) = (8 ; 18)$.
3. Soit $(x ; y)$ un couple d'entiers relatifs.
On a : $34x - 15y = 0 \Leftrightarrow 34(x + x_0) - 15(y + y_0) = 2$.
On en déduit que les solutions de (E) sont les couples $(x + x_0 ; y + y_0)$ où $(x ; y)$ est solution de (E').
L'ensemble des solutions de (E) est donc : $\{(15k + 8 ; 34k + 18), k \in \mathbb{Z}\}$.

Systèmes

1. Résoudre dans $\mathbb{Z}$ le système (S_1) : $\begin{cases} x \equiv -1 \ [34] \\ x \equiv 1 \ [15] \end{cases}$.

Solution

Soit x une solution de (S_1). Il existe deux entiers relatifs p et q tels que : $x = 34p - 1$ et $x = 15q + 1$.
On en déduit que : $34p - 15q = 2$.
D'après l'étude précédente, il existe un entier relatif k tel que : $(p ; q) = (15k + 8 ; 34k + 18)$.
Réciproquement, soit k un entier relatif.
Posons : $x = 34(15k + 8) - 1$.
On a : $x \equiv -1 \ [34]$ et $x \equiv 1 \ [15]$.
L'ensemble des solutions de (S_1) est donc : $\{510k + 271, k \in \mathbb{Z}\}$.
[À noter qu'on obtient le même résultat en posant : $x = 15(34k + 18) + 1$.]

2. Résoudre dans $\mathbb{N}^2$ le système (S_2) : $\begin{cases} \text{PGCD}(x ; y) = 12 \\ x + y = 60 \end{cases}$.

Solution

$\begin{cases} \text{PGCD}(x ; y) = 12 \\ x + y = 60 \end{cases} \Leftrightarrow \begin{cases} x = 12x' \text{ et } y = 12y' \\ \text{PGCD}(x' ; y') = 1 \\ x' + y' = 5 \end{cases}$.

On obtient : $x' = 1$ et $y' = 4$; $x' = 2$ et $y' = 3$; $x' = 3$ et $y' = 2$; $x' = 4$ et $y' = 1$.
L'ensemble des solutions de (S_2) est donc : $\{(12 ; 48), (24 ; 36), (36 ; 24), (48 ; 12)\}$.

Exercices

3.a Déterminer le PPCM des entiers relatifs a et b dans chacun des cas suivants.

- $a = 48$ et $b = 12$
- $a = -3$ et $b = 8$
- $a = 15$ et $b = 21$
- $a = 160$ et $b = 200$.

3.b Déterminer le PGCD des entiers relatifs a et b dans chacun des cas suivants.

- $a = 24$ et $b = 24$
- $a = 14$ et $b = 31$
- $a = -75$ et $b = -25$
- $a = 132$ et $b = -96$.

3.c À l'aide de l'algorithme d'Euclide, déterminer le PGCD de 2 867 et 3 431.

3.d Démontrer que deux nombres impairs consécutifs sont premiers entre eux.

3.e À l'aide du théorème de Bézout, démontrer que : $\forall n \in \mathbb{Z}$, PGCD$(2n + 1 ; 3n + 1) = 1$.

3.f Démontrer que le produit de trois entiers relatifs consécutifs est divisible par 6.

3.g Dans chacun des cas suivants, déterminer le PGCD des entiers relatifs a et b, puis en déduire leur PPCM.

- $a = 24$ et $b = 56$
- $a = 300$ et $b = 750$
- $a = 1\,386$ et $b = 546$
- $a = -3\,015$ et $b = 3\,975$.

4 Nombres premiers

4.1. Généralités

Définition et propriété

Définition

On dit qu'un entier naturel p est premier s'il possède exactement deux diviseurs positifs : 1 et p.

Exemples

- 2, 3, 5, 7, 11 et 13 sont des nombres premiers.
- 12 et 49 ne sont pas des nombres premiers.

Remarques

- *0 et 1 ne sont pas des nombres premiers.*
- *Deux nombres premiers distincts sont premiers entre eux.*

Propriété

Tout entier naturel n différent de 0 et de 1 admet au moins un diviseur premier.

Démonstration

Considérons l'ensemble A défini par : $A = \{d \in \mathcal{D}(n), d \geq 2\}$.

$n \in A$; donc A, partie non vide de $\mathbb{N}$, admet un plus petit élément p.

Le nombre p, comme tous les éléments de A, est un entier naturel différent de 0 et de 1.

On en déduit que p est un nombre premier ; en effet si ce n'était pas le cas, il admettrait un diviseur q entier naturel autre que 1 ou lui-même et q serait un élément de A strictement plus petit que p.

L'ensemble des nombres premiers

L'algorithme suivant, dû à Ératosthène de Cyrène (276-194 av. J.-C.), permet de déterminer les nombres premiers inférieurs à un nombre donné n. On écrit les entiers naturels successifs compris entre 1 et n.

- On barre 1 qui n'est pas premier.
- Le nombre 2 est premier. On barre tous les multiples de 2 autres que 2.
- Le premier nombre non barré est 3, qui est donc premier.

On barre tous les multiples de 3 autres que 3.

- On itère le procédé jusqu'à la fin du tableau.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Propriété 1

Il existe une infinité de nombres premiers.

Démonstration

Supposons qu'il n'existe qu'un nombre fini de nombres premiers distincts notés $p_1, p_2, \dots, p_s$ et considérons le nombre n défini par : $n = p_1 \times p_2 \times \dots \times p_s + 1$.

D'après la propriété précédente, n admet au moins un diviseur premier p.

Donc p est l'un des nombres $p_1, p_2, \dots, p_s$.

On en déduit que p divise $n - p_1 \times p_2 \times \dots \times p_s$, c'est-à-dire 1.

Ce qui est contradictoire avec le fait que p est premier.

Il existe donc une infinité de nombres premiers.

Remarque

Depuis l'Antiquité, les mathématiciens s'interrogent sur la répartition des nombres premiers. Est-elle régulière ? Présente-t-elle des particularités ?

- *Jacques Hadamard a démontré en 1896 qu'il y a environ $\frac{n}{\ln(n)}$ nombres premiers inférieurs à n et que cette approximation est d'autant plus précise que n est grand.*
- *En 1963, Stanislas Ulam place les entiers naturels en spirale, comme l'indique la figure ci-contre, puis noircit les cases des nombres non premiers.*
Il obtient une constellation présentant des alignements surprenants, appelée spirale d'Ulam (cf. introduction du chapitre).
- *Le plus grand nombre premier connu, depuis 1998, est : $2^{3\,021\,377} - 1$.*

4	5	6
3	0	7
2	1	8

Propriété 2

Tout entier naturel n, autre que 0 et 1 et non premier, admet au moins un diviseur premier d tel que : $1 < d^2 \leq n$.

Démonstration

Si n est un entier naturel non premier, autre que 0 et 1, il admet au moins un diviseur strictement compris entre 1 et n. Notons d le plus petit d'entre eux.

On a : $n = d \times d'$, avec $1 < d \leq d'$; donc : $1 < d^2 \leq n$.

De plus d est premier (sinon il ne serait pas le plus petit diviseur strictement positif de n).

Cette propriété fournit un critère d'arrêt lorsqu'on cherche à savoir si un entier naturel est premier.

M Pour déterminer si un entier naturel n est premier, on essaie de le diviser par tous les nombres premiers inférieurs à $\sqrt{n}$. Si aucun de ces nombres ne divise n, on peut dire que n est premier.

Exemple

Démontrer que 137 est un nombre premier.
On a : $\sqrt{137} \approx 11{,}704$.
137 n'est divisible par aucun des nombres premiers 2, 3, 5, 7, 11 ; de plus, $13^2 > 137$.
Donc 137 est un nombre premier.

4.2. Décomposition en produit de facteurs premiers

Théorème fondamental

Considérons l'entier naturel 14 394 744.
Il peut se décomposer en produit de facteurs premiers ; en effet : $14\,394\,744 = 2^3 \times 3^2 \times 7 \times 13^4$.

Plus généralement, nous admettons le théorème fondamental suivant.

Théorème

Soit n entier naturel ($n \geq 2$).
- **Il existe des nombres premiers $p_1, p_2, \dots, p_k$ et des entiers naturels non nuls $\alpha_1, \alpha_2, \dots, \alpha_k$ tels que :**
$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k} \quad \text{et} \quad p_1 < p_2 < \dots < p_k.$$
- **Cette décomposition est unique.**

Exemple

Pour décomposer 4 872 en produit de facteurs premiers, on peut utiliser la disposition pratique ci-contre.
On obtient : $4\,872 = 2^3 \times 3 \times 7 \times 29$.

4 872	2
2 436	2
1 218	2
609	3
203	7
29	29
1	

Exemples d'utilisation

1. *Détermination de PPCM et de PGCD*
Déterminer le PPCM et le PGCD de 700 et 18 375.

Solution

On a : $700 = 2^2 \times 5^2 \times 7$ et $18\,375 = 3 \times 5^3 \times 7^2$.
Donc : $\text{PPCM}(700 ; 18\,375) = 2^2 \times 3 \times 5^3 \times 7^2 = 73\,500$.
$\text{PGCD}(700 ; 18\,375) = 5^2 \times 7 = 175$.

2. *Détermination de l'ensemble des diviseurs positifs d'un entier naturel*
***a)* Quel est le nombre de diviseurs positifs de 14 553 ?**
***b)* Déterminer l'ensemble $\mathcal{D}$ des diviseurs positifs de 14 553.**

Solution

a) On a : $14\,553 = 3^3 \times 7^2 \times 11$.
Les diviseurs positifs de 14 553 sont les nombres qui peuvent s'écrire sous la forme $3^\alpha \times 7^\beta \times 11^\gamma$, où $\alpha \in \{0 ; 1 ; 2 ; 3\}$, $\beta \in \{0 ; 1 ; 2\}$ et $\gamma \in \{0 ; 1\}$.
Le nombre de diviseurs positifs de 14 553 est donc : $4 \times 3 \times 2 = 24$.

3^α	1	3	9	27
7^β	1	7	49	
11^γ	1	11		

b) Chaque diviseur positif de 14 553 est le produit de 3 nombres, à raison d'un par chacune des trois lignes du tableau ci-contre.
On en déduit que les diviseurs positifs de 14 553 sont :

$1 \times 1 \times 1$	$1 \times 1 \times 11$	$1 \times 7 \times 1$	$1 \times 7 \times 11$	$1 \times 49 \times 1$	$1 \times 49 \times 11$
$3 \times 1 \times 1$	$3 \times 1 \times 11$	$3 \times 7 \times 1$	$3 \times 7 \times 11$	$3 \times 49 \times 1$	$3 \times 49 \times 11$
$9 \times 1 \times 1$	$9 \times 1 \times 11$	$9 \times 7 \times 1$	$9 \times 7 \times 11$	$9 \times 49 \times 1$	$9 \times 49 \times 11$
$27 \times 1 \times 1$	$27 \times 1 \times 11$	$27 \times 7 \times 1$	$27 \times 7 \times 11$	$27 \times 49 \times 1$	$27 \times 49 \times 11$.

Donc : $\mathcal{D} = \{1 ; 3 ; 7 ; 9 ; 11 ; 21 ; 27 ; 33 ; 49 ; 63 ; 77 ; 99 ; 147 ; 189 ; 231 ; 297 ; 441 ; 539 ; 693 ; 1\,323 ; 1\,617 ; 2\,079 ; 4\,851 ; 14\,553\}$.

4.3. Travaux dirigés

Le petit théorème de Fermat[3]

Soit p un nombre premier.

1°) *a)* Démontrer que pour tout entier naturel i strictement compris entre 0 et p, C_p^i est multiple de p.
***b)* En déduire que pour tous entiers relatifs a et b, on a : $(a+b)^p \equiv a^p + b^p$ [p].**

2°) *a)* Démontrer que : $\forall\, a \in \mathbb{N}$, $a^p \equiv a$ [p].
***b)* En déduire que pour tout entier naturel a premier avec p, on a : $a^{p-1} \equiv 1$ [p].**

Solution

1°) *a)* On a : $C_p^i = \dfrac{p!}{i!(p-i)!} = \dfrac{p}{i} \times \dfrac{(p-1)!}{(i-1)!\,(p-i)!} = \dfrac{p}{i} C_{p-1}^{i-1}$; donc : $pC_{p-1}^{i-1} = iC_p^i$.

p divise iC_p^i et est premier avec i ; donc C_p^i est multiple de p.

b) On a : $(a+b)^p = a^p + \left(\sum_{i=1}^{p-1} C_p^i\, a^i b^{p-i}\right) + b^p$.

Or : $\sum_{i=1}^{p-1} C_p^i\, a^i b^{p-i} \equiv 0$ [p] ; donc : $(a+b)^p \equiv a^p + b^p$ [p].

2°) *a)* Pour tout entier naturel a, considérons la proposition P(a) : « $a^p \equiv a$ [p] ».

- P(0) est vraie.
- Soit k un entier naturel.

Si P(k) est vraie, on a : $k^p \equiv k$ [p].

Or, d'après la question précédente, on a : $(k+1)^p \equiv k^p + 1^p$ [p].

Donc : $(k+1)^p \equiv k+1$ [p] ; c'est-à-dire : P($k+1$) est vraie.

On en déduit que P(a) est vraie pour tout entier naturel a.

b) Soit a un entier naturel premier avec p.

On a : $a \times a^{p-1} \equiv a \times 1$ [p] ; donc : $a^{p-1} \equiv 1$ [p].

Les propriétés démontrées à la question 2 sont connues sous le nom de petit théorème de Fermat.

Exercices

4.a Vérifier si les nombres suivants sont premiers : 103 ; 119 ; 137 ; 211.

4.b *a)* Pour tout entier naturel n non multiple de 5, le nombre $6n + 5$ est-il premier ?
b) Pour tout entier naturel n, le nombre $n^2 - n + 41$ est-il premier ?

4.c Décomposer en produit de facteurs premiers les nombres suivants : 120 ; 126 ; 336 ; 735.

4.d En utilisant la décomposition en produit de facteurs premiers, mettre les fractions suivantes sous forme irréductible :

$$\frac{495}{315} \ ; \ \frac{780}{204} \ ; \ \frac{918}{1\,242}.$$

4.e En utilisant la décomposition en produit de facteurs premiers, dresser la liste des diviseurs des nombres suivants : 90 ; 120 ; 245.

4.f Dans chacun des cas suivants, décomposer a et b en produits de facteurs premiers et déterminer leur PGCD et leur PPCM.

- $a = 4\,312$ et $b = 6\,776$
- $a = 28\,665$ et $b = 412\,375$.

4.g Décomposer 1 925 et 6 860 en produit de facteurs premiers, puis calculer :

$$\frac{51}{1\,925} + \frac{3}{6\,860}.$$

3 *Pierre de Fermat, mathématicien français – 1601 - 1665.*

Exercices

APPRENTISSAGE

Raisonnement par récurrence

1 Démontrer que pour tout entier naturel n non nul, on a :

a) $\sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3}$

b) $\sum_{k=1}^{n} k(k+1)(k+2) = \frac{n(n+1)(n+2)(n+3)}{4}$.

2 Démontrer que pour tout entier naturel n non nul, on a :

a) $\sum_{k=1}^{n} k(n-k) = \frac{(n-1)n(n+1)}{6}$

b) $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$

c) $\sum_{k=1}^{n} k2^{k-1} = (n-1)2^n + 1$.

3 Démontrer que pour tout entier naturel n supérieur ou égal à 5, on a : $2^n > 5(n+1)$.

4 Démontrer que n droites du plan déterminent au maximum $\frac{n(n+1)}{2} + 1$ régions.

5 Soit a et b deux nombres réels.
a) Démontrer que pour tout entier n supérieur ou égal à 2, on a :
$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$.
b) En déduire que pour tout entier n impair et supérieur à 2, on a :
$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \ldots - ab^{n-2} + b^{n-1})$.

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

6 Résoudre dans $\mathbb{Z}^2$ le système : $\begin{cases} xy = -1 \\ 2x + y^3 = 1 \end{cases}$.

7 Effectuer la division euclidienne de a par b dans chacun des cas suivants.
- $a = -2\,372$ et $b = 44$
- $a = 735$ et $b = -412$
- $a = -235$ et $b = -17$
- $a = 50\,764$ et $b = 327$.

8 La division euclidienne de 900 par un entier naturel b a pour quotient 14 et pour reste r. Quelles sont les valeurs possibles de b et r ?

9 Déterminer les entiers naturels n dont la division euclidienne par 16 a un reste égal au carré du quotient.

10 Soit q et r le quotient et le reste de la division euclidienne d'un entier naturel a par un entier naturel b. Sachant que $a + b + r = 3\,025$ et $q = 50$, rétablir la division.

11 Écrire en base deux les nombres suivants : 85 ; 104 ; 3 607.

12 Écrire dans le système décimal les nombres suivants, écrits en base deux :
$\overline{10110}^2$; $\overline{111000}^2$; $\overline{10101010}^2$; $\overline{110100011}^2$.

13 Écrire $2^6 - 1$ en base deux.

14 b est un entier naturel supérieur à 1.
Écrire $(b+1)^2$ en base b.
(On distinguera deux cas : $b = 2$ et $b \neq 2$.)

Multiples et diviseurs

15 Résoudre dans $\mathbb{Z}$ l'équation : $x^2 \equiv -1$ [5].

16 Résoudre dans $\mathbb{Z}$ l'équation :
$x^2 - 3x + 4 \equiv 0$ [7].

17 Démontrer que la somme des cubes de trois entiers relatifs consécutifs est divisible par 9.

18 1. Déterminer, suivant les valeurs de l'entier naturel n, le reste de la division euclidienne par 7 du nombre $A = n^2 - n + 1$.
2. En déduire les entiers n tels que le nombre A soit divisible par 7.
3. Déterminer le reste de la division euclidienne par 7 du nombre $B = (2\,753)^2 - 2\,753 + 1$.

19 Démontrer que pour tous entiers naturels a, b et c, on a : $a^3 + b^3 + c^3 \equiv 0$ [7] $\Rightarrow$ $abc \equiv 0$ [7].

20 1. Déterminer le reste de la division euclidienne de $11^{1\,999}$ par 7.
2. Plus généralement, déterminer suivant les valeurs de l'entier naturel n, le reste de la division euclidienne de 11^n par 7.

21 Déterminer les entiers relatifs n tels que la fraction $\frac{n+17}{n-1}$ soit un entier relatif.

22 Démontrer que pour tout entier naturel n, le nombre $n(2n+1)(7n+1)$ est divisible par 2 et par 3.

23 p et q sont deux entiers naturels inférieurs ou égaux à 9. Parmi les nombres suivants, un seul est divisible par 7 quelles que soient les valeurs de p et q. Trouver ce nombre.

a) $\overline{qqp\ pqp}^{10}$ b) $\overline{qqq\ ppp}^{10}$
c) $\overline{qpq\ qpp}^{10}$ d) $\overline{qpq\ pqp}^{10}$.

24 1. Un nombre s'écrit $\overline{x43y}$ dans le système décimal.
Déterminer x et y pour qu'il soit divisible par 2 et 9.
2. Un nombre s'écrit $\overline{28x75y}$ dans le système décimal.
Déterminer x et y pour qu'il soit divisible par 3 et 11.
3. Un nombre s'écrit $\overline{1x1yxy}$ dans le système décimal.
Déterminer x et y pour qu'il soit divisible par 63.

25 Démontrer que pour tout entier naturel n, on a :
a) $3^{2n+1} + 2^{n+2}$ divisible par 7
b) $9^{n+1} + 2^{6n+1}$ divisible par 11
c) $10^{9n+2} + 10^{6n+1} + 1$ divisible par 111.
(On pourra faire un raisonnement par récurrence.)

26 Démontrer que pour tout entier naturel n, on a :
a) $5^{2n} - 3^n$ divisible par 11
b) $7^n - 1$ divisible par 6
c) $3^{2n} - 2^n$ divisible par 7
d) $3 \times 5^{2n+1} + 2^{3n+1}$ divisible par 17.
(On pourra utiliser les congruences.)

27 Soit n un entier non divisible par 7.
Démontrer que l'un des nombres $n^3 - 1$ et $n^3 + 1$ est divisible par 7.

28 Soit n un entier naturel.
1. Quels sont les restes possibles de la division euclidienne de n^4 par 5 ?
2. Démontrer que $n^5 - n$ est divisible par 5.

29 Soit n un entier naturel.
1. Déterminer suivant les valeurs de n le reste de la division euclidienne de 7^n par 10.
2. Dans le système décimal, déterminer suivant les valeurs de n le chiffre des unités du nombre :
$$A = 1 + 7 + 7^2 + 7^3 + \ldots + 7^n.$$

30 Quels sont les entiers naturels n pour lesquels $15 \times 3^n - 3$ est divisible par 7 ?

31 Démontrer que parmi cinq entiers relatifs, on peut toujours en choisir trois dont la somme est divisible par 3.

PGCD et PPCM
Nombres premiers entre eux

32 Déterminer le PPCM des entiers a et b dans chacun des cas suivants.
- $a = 24$ et $b = 56$
- $a = 180$ et $b = 450$.

33 Déterminer le PGCD des entiers a et b dans chacun des cas suivants.
- $a = 48$ et $b = 32$
- $a = 1\,640$ et $b = 492$
- $a = 168$ et $b = 2\,160$
- $a = 343$ et $b = 1\,225$.

34 Déterminer les couples $(a ; b)$ d'entiers naturels tels que : PGCD$(a ; b) = 7$ et $a + b = 105$.

35 Déterminer le PGCD des entiers a et b dans chacun des cas suivants.
- $a = 1\,455$ et $b = 335$
- $a = 3\,604$ et $b = 4\,452$
- $a = 13\,860$ et $b = 4\,438$
- $a = 323\,232$ et $b = 232\,323$.

36 Déterminer le PPCM des entiers a et b dans chacun des cas suivants.
- $a = 162$ et $b = 252$
- $a = 6\,974$ et $b = 9\,287$.

37 Résoudre dans $\mathbb{N}^2$ les systèmes suivants.
a) $\begin{cases} \text{PGCD}(x ; y) = 354 \\ x + y = 5\,664 \end{cases}$ *b)* $\begin{cases} \text{PPCM}(x ; y) = 168. \\ x \times y = 1\,008 \end{cases}$

38 Pour tout couple $(a ; b)$ d'entiers naturels, on désigne par μ leur PPCM et par δ leur PGCD.
1. Déterminer les couples $(a ; b)$ d'entiers naturels tels que : $2\mu + 3\delta = 11$.
2. Dresser la liste des diviseurs de 108.
Déterminer les couples $(a ; b)$ d'entiers naturels tels que : $\mu - 3\delta = 108$ et $10 < \delta < 15$.

39 1. Quels sont les entiers naturels dont le carré est un diviseur de 1998 ?
2. Pour tout couple $(a ; b)$ d'entiers naturels, on désigne par μ leur PPCM et par δ leur PGCD.
Déterminer les couples $(a ; b)$ d'entiers naturels tels que :
$$\mu^2 - 3\delta^2 = 1998.$$

40 Démontrer que pour tout entier naturel n, on a :
- $n^2(n^2 - 1)$ divisible par 12 ;
- $n^2(n^4 - 1)$ divisible par 60 ;
- $n(n^6 - 1)$ divisible par 42.

41 Démontrer que les fractions suivantes sont irréductibles.
a) $\dfrac{n}{2n+1}$ $(n \in \mathbb{Z})$ *b)* $\dfrac{7n+3}{5n+2}$ $(n \in \mathbb{Z})$
c) $\dfrac{n^2}{n+1}$ $(n \in \mathbb{Z} \setminus \{-1\})$ *d)* $\dfrac{2n(n+1)}{2n+1}$ $(n \in \mathbb{Z})$.

42 Démontrer que si la fraction $\dfrac{a}{b}$ est irréductible, il en est de même pour les fractions :
$$\frac{a+b}{ab} \qquad \frac{ab}{a^2+b^2} \qquad \frac{a+b}{a^2+ab+b^2} \qquad \frac{a^2b^2}{a^2+b^2}$$

43 1. Déterminer l'ensemble des entiers relatifs n tels que $n + 2$ divise $2n - 1$.
2. Démontrer que pour tout entier relatif n, les nombres $n + 2$ et $2n^2 + 3n - 1$ sont premiers entre eux.
3. En déduire les entiers relatifs n pour lesquels la fraction $\dfrac{(2n-1)(2n^2+3n-1)}{(n^2-2)(n+2)}$ est un entier relatif.

44 1. Résoudre dans $\mathbb{Z}^2$ l'équation (E') :
$$2x - 3y = 0.$$
2. Déterminer dans $\mathbb{Z}^2$ une solution de l'équation (E) :
$$2x - 3y = 3.$$
3. Résoudre (E).

45 Résoudre dans $\mathbb{Z}^2$ l'équation : $x + 11y = 203$.

46 1. En utilisant l'algorithme d'Euclide, déterminer deux entiers naturels x et y tels que :
$$45x - 28y = 1.$$
2. Résoudre dans $\mathbb{Z}^2$ l'équation (E) : $45x - 28y = 1$.
3. Résoudre dans $\mathbb{Z}^2$ l'équation (E') : $45x - 28y = 6$.

47 Un entier naturel n a :
– pour reste 5 dans la division euclidienne par 8,
– pour reste 4 dans la division euclidienne par 11.
Quel est le reste de la division euclidienne de n par 88 ?

48 Résoudre dans $\mathbb{Z}$ le système : $\begin{cases} x \equiv 1 \ [3] \\ x \equiv 2 \ [7] \end{cases}$.

Nombres premiers

49 Vérifier si les nombres suivants sont premiers : 649 ; 1 001 ; 1 999 ; 71 487 ; 257 323.

50 Démontrer que si n est un entier naturel supérieur ou égal à 3, alors $n^2 + 4n - 5$ est un nombre qui n'est jamais premier.

51 Soit A = 100!.
1. Quelle est la puissance de 2 dans la factorisation de A ?
2. Par combien de zéros A se termine-t-il ?

52 Déterminer les entiers naturels n tels que :
a) PPCM(n ; 6) = 96 ; *b)* PPCM(n ; 72) = 216.

53 Déterminer l'entier naturel n tel que :
$600 < n < 1\,100$ et PGCD(n ; 630) = 105.

54 Quel est le plus petit entier naturel ayant 15 diviseurs positifs ?

55 Déterminer les entiers naturels, écrits avec deux chiffres, dont le nombre de diviseurs est le plus grand possible.

56 Déterminer l'ensemble des entiers naturels n tels que n, $n + 2$, $n + 6$, $n + 8$, $n + 12$ et $n + 14$ soient premiers.

57 Déterminer l'entier naturel n, écrit avec 4 chiffres, tel que les restes des divisions euclidiennes de 39 818 et 62 566 par n sont respectivement 37 et 53.

58 Démontrer qu'un entier naturel n possède un nombre impair de diviseurs positifs si et seulement si n est un carré parfait.

59 Déterminer les couples $(a ; b)$ d'entiers naturels tels que : PPCM(a ; b) = 504 et $a + b = 135$.

60 Déterminer les couples $(a ; b)$ d'entiers naturels tels que : PGCD(a ; b) = 42 et PPCM(a ; b) = 1 680.

61 1. Décomposer 469 en produit de facteurs premiers.
2. Résoudre dans $\mathbb{N}^2$ l'équation : $x^3 - y^3 = 469$.

APPROFONDISSEMENT

62 Soit a, b et c trois entiers naturels non nuls. Démontrer que si $ab < c$, alors : $a + b \leq c$.

63 On se propose de résoudre dans $\mathbb{Z}$ l'équation (E) : $x^2 \equiv -1$ [25].
1. Démontrer que (E) se ramène à chercher des nombres x tels que : $x^2 = 49 + 25k$ ($k \in \mathbb{Z}$).
2. Résoudre alors l'équation (E).

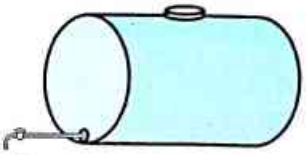
64 Soit a et b deux entiers naturels non nuls. Démontrer que : PGCD($13a + 8b$; $5a + 3b$) = PGCD(a ; b).

65 Soit n un entier relatif.
Démontrer que si 11 ne divise pas $(n - 4)$, alors $(2n + 3)$ et $(n + 7)$ sont premiers entre eux.

66 On veut planter des arbres sur le périmètre d'un terrain triangulaire de côtés 132 m, 156 m et 204 m, de telle sorte qu'il y ait un arbre à chaque sommet du triangle et que les arbres soient également espacés. Quel est le nombre minimum d'arbres que l'on pourra planter si l'on veut que la distance entre deux arbres soit exprimée en un nombre entier de mètres ?

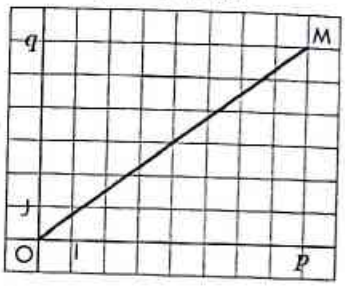
67 On dispose de dix poids, dont les masses respectives sont 1, 2, 2^2, 2^3, ... , 2^8 et 2^9 grammes.
1. Quelle est la masse maximale M que l'on peut équilibrer sur une balance avec ces dix poids ?
2. Démontrer que tout objet, dont la masse est un nombre entier de grammes inférieur ou égal à M, peut être équilibré avec ces dix poids.

68 À l'aide de deux seaux dont les capacités en litres sont C_1 et C_2, on veut mettre exactement 1 litre d'eau dans une citerne que l'on peut remplir ou vider à volonté.



1. Est-ce possible lorsque $C_1 = 7$ et $C_2 = 4$?
Lorsque $C_1 = 6$ et $C_2 = 4$?
2. Étudier le cas général.

69 Le plan est muni du repère (O, I, J).
Soit p et q deux entiers naturels non nuls et M le point de coordonnées $(p ; q)$.
Déterminer, en fonction de p et q, le nombre de points du segment [OM] dont les coordonnées sont des entiers naturels.



70 Soit a, b et c trois entiers naturels tels que :
$$a^2 + b^2 = c^2.$$
Démontrer que abc est divisible par 60.

71 On désigne par $\varphi(n)$ le nombre d'entiers naturels inférieurs à n et premiers avec n.
1. Calculer $\varphi(5)$, $\varphi(13)$, $\varphi(15)$, $\varphi(36)$.
2. p et q sont deux nombres premiers distincts. Calculer $\varphi(p)$, $\varphi(pq)$, $\varphi(p^2)$.

72 Soit (x_n) et (y_n) les suites définies par :

$$\begin{cases} x_0 = 3,\ y_0 = 1 \\ \forall n \in \mathbb{N},\ x_{n+1} = \dfrac{6}{5}x_n + \dfrac{2}{5}y_n + 1 \\ \forall n \in \mathbb{N},\ y_{n+1} = \dfrac{2}{5}x_n + \dfrac{9}{5}y_n + 2 \end{cases}.$$

1. Démontrer par récurrence que les points M_n de coordonnées $(x_n ; y_n)$ sont sur la droite (D) d'équation :
$$2x - y - 5 = 0.$$
2. En déduire x_{n+1} en fonction de x_n.
3. Démontrer que (x_n) et (y_n) sont des suites d'entiers relatifs.
4. Soit n un entier naturel.
a) Démontrer que x_n est divisible par 5 si et seulement si y_n est divisible par 5.

b) Démontrer que si x_n et y_n ne sont pas divisibles par 5, alors ils sont premiers entre eux.

5. *a)* Démontrer par récurrence que :

$$\forall\, n \in \mathbb{N},\ x_n = 2^{n+1} + 1.$$

b) Soit n un entier naturel. Démontrer que 5 divise x_n si et seulement si 5 divise x_{n+4}.

c) En déduire les valeurs de n pour lesquelles x_n et y_n sont divisibles par 5.

73 On considère les nombres A et B tels que :

$$A = 10^{6n+2} + 10^{3n+1} + 1$$
$$B = 10^{9n} + 10^{6n} + 10^{3n} + 1 \quad (n \in \mathbb{N}).$$

1. Vérifier que : $10^3 - 1 = 9 \times 111$;
$10^3 + 1 = 7 \times 11 \times 13$.

2. Démontrer que :
- $\forall\, n \in \mathbb{N}$, A est divisible par 111 ;
- si n est impair, alors A est divisible par 7 et par 13.

3. *a)* Si n est impair, démontrer que B est divisible par 7, 11 et 13.

b) Si n est pair, déterminer le reste de la division euclidienne de B par 7, 11, 13 et 111.

74 1. Résoudre dans $\mathbb{Z}^2$ l'équation :

$$661x - 991y = 1.$$

2. Soit (u_n) et (v_n) les suites arithmétiques définies par :

$$\begin{cases} u_0 = 3,\ v_0 = 2 \\ \forall\, n \in \mathbb{N},\ u_{n+1} = u_n + 991 \\ \forall\, n \in \mathbb{N},\ v_{n+1} = v_n + 661 \end{cases}.$$

Déterminer tous les couples $(p\,;\,q)$ d'entiers naturels inférieurs à 2 000, tels que : $u_p = v_q$.

75 Soit à résoudre dans $\mathbb{N}^2$ l'équation

$$(E) : 15x^2 - 7y^2 = 9.$$

1. *a)* Démontrer que dans le système décimal, le dernier chiffre d'un carré est 1, 4, 5, 6 ou 9.

b) En déduire que $7y^2 + 9$ n'est pas divisible par 5.

2. Résoudre l'équation (E).

76 Soit à résoudre dans $\mathbb{Z}^2$ l'équation

$$(E) : 3x^2 + 3x + 7 = y^3.$$

1. Vérifier que (E) est équivalente à :

$$3(x^2 + x + 2) = y^3 - 1.$$

2. Résoudre l'équation (E).

(On pourra distinguer 3 cas :

$$y \equiv 0\ [3],\quad y \equiv 1\ [3] \quad \text{et} \quad y \equiv 2\ [3].)$$

77 On désigne par $\mathbb{P}$ l'ensemble des entiers naturels premiers. On se propose de résoudre dans $\mathbb{P}^2$ l'équation (E) $x^2 - y^2 = pq$, où p et q sont deux entiers naturels premiers.

1. Étudier le cas où $p = q = 2$.

2. Étudier le cas où $q = 2$ et $p > 2$.

3. *a)* On suppose que : $2 < q \leq p$.
- Démontrer que y est nécessairement égal à 2.
- En déduire que si $p - q \neq 4$, (E) n'a pas de solution.

b) On suppose que : $p - q = 4$.

Démontrer que si $(x\,;\,2)$ est solution de (E), alors les nombres q, x et p forment une suite arithmétique de raison 2.

En déduire que (E) n'a de solution que si $q = 3$ et $p = 7$.

(On pourra démontrer que pour tout entier n, l'un des trois nombres n, $n + 2$, $n + 4$ est divisible par 3.)

Quelle est la solution de (E) dans ce cas ?

78 On se propose de résoudre dans $\mathbb{N}^2$ l'équation

$$(E) : 5^x - 4^x = y^2.$$

1. Vérifier que $(1\,;\,1)$ est solution de (E).

Dans la suite du problème, on suppose que x est différent de 1.

2. L'objet de cette question est de démontrer que x est pair.

a) Quels sont les entiers naturels n tels que : $n^2 \equiv 5\ [8]$?

b) Démontrer que si x est impair, alors $5^x - 4^x \equiv 5\ [8]$.

c) Conclure.

3. On pose : $x = 2m$ $(m \in \mathbb{N})$.

a) Démontrer que (E) est équivalente à :

$$(5^m - y)(5^m + y) = 2^{4m}.$$

b) En déduire qu'il existe deux entiers p et q tels que :

$$5^m - y = 2^p \quad \text{et} \quad 5^m + y = 2^q, \text{ avec } p + q = 4m.$$

c) Déduire de 3. *b)* que : $\begin{cases} p = 1 \\ q = 4m - 1 \\ 5^m = 1 + 4^{2m-1} \end{cases}$.

En déduire que : $m \leq 1$.

(On pourra faire un raisonnement par l'absurde.)

4. Déterminer les solutions de (E).

79 On se propose de déterminer tous les entiers relatifs k tels que $k^4 + k^3 + k^2 + k + 1$ soit un carré parfait.

On pose : $q^2 = k^4 + k^3 + k^2 + k + 1$ $(q \in \mathbb{Z})$.

1. Établir les égalités suivantes :

$$4q^2 = (2k^2 + k)^2 + 3k^2 + 4k + 4 \quad (1)$$
$$4q^2 = (2k^2 + k + 1)^2 - (k - 3)(k + 1) \quad (2)$$
$$4q^2 = (2k^2 + k + 2)^2 - 5k^2 \quad (3).$$

2. Déduire de (1) et (3) que :

$$(2k^2 + k)^2 < 4q^2 \leq (2k^2 + k + 2)^2.$$

3. Déduire de la question 2. que :

$$4q^2 = (2k^2 + k + 1)^2 \quad (4)$$

ou

$$4q^2 = (2k^2 + k + 2)^2 \quad (5).$$

4. Déterminer les valeurs de k en considérant les égalités (2) et (4), (3) et (5).

80 1. Soit p et q deux entiers relatifs premiers entre eux, n un entier naturel non nul.

Démontrer que p et q^n sont premiers entre eux.

2. Soit $P(x) = a_n x^n + \ldots + a_1 x + a_0$ un polynôme à coefficients entiers relatifs admettant une racine rationnelle $\frac{p}{q}$ (p et q sont des entiers relatifs premiers entre eux).

Démontrer que p divise a_0 et q divise a_n.

3. Factoriser le polynôme : $3x^3 + 7x^2 + 7x + 4$.

4. Résoudre dans $\mathbb{Q}$ l'équation :

$$x^5 + 127x^4 - 12x^3 + x^2 + 7x - 1 = 0.$$

81 1. Soit n un entier naturel congru à 3 modulo 4.

Démontrer que n admet un diviseur premier congru à 3 modulo 4.

(On pourra remarquer qu'un produit de nombres congrus à 1 modulo 4 est congru à 1 modulo 4.)

2. Démontrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

(On pourra utiliser un nombre n de la forme $2 \times p! - 1$.)

82 On appelle nombre triangulaire tout entier naturel qui peut s'écrire sous la forme $\frac{a^2 + a}{2}$ $(a \in \mathbb{N})$.

1. Démontrer que si n est la somme de deux nombres triangulaires, alors $4n + 1$ est la somme de deux carrés.
2. Étudier la réciproque.

83 Nombres amiables – Nombres parfaits

1. On appelle diviseur strict d'un entier naturel n tout diviseur de n positif et autre que lui-même.
Déterminer les diviseurs stricts de 220.
2. On appelle nombres amiables deux entiers naturels tels que chacun d'eux est égal à la somme des diviseurs stricts de l'autre.
Vérifier que : 220 et 284 sont amiables ;
17 296 et 18 416 sont amiables.
3. On appelle nombre parfait tout entier naturel égal à la somme de ses diviseurs stricts (c'est-à-dire amiable avec lui-même).
a) Le nombre 28 est-il parfait ?
b) Déterminer un nombre premier p tel que 2^4p soit un nombre parfait.
c) Soit n et p deux entiers naturels, tels que p soit premier. Quelle doit être l'expression de p en fonction de n pour que 2^np soit parfait ?
Dresser la liste des nombres parfaits de cette forme, pour $n < 10$.

84 Nombres de Mersenne

1. Soit a et n deux entiers naturels supérieurs ou égaux à 2. Démontrer que si $a^n - 1$ est premier, alors $a = 2$ et n est premier.
2. On appelle nombre de Mersenne, tout entier naturel M_n de la forme $M_n = 2^n - 1$, où n est un entier naturel premier.
a) Vérifier que M_2, M_3, M_5 et M_7 sont premiers.
b) Qu'en est-il de M_{11} ?

Le Père Marin Mersenne (1558–1648) fut le premier à tenter de dresser la liste des nombres premiers de la forme $2^n - 1$.
Il le fit, avec quelques erreurs, jusqu'à $n = 257$.
On sait aujourd'hui que, jusqu'à $n = 5\,000$, $2^n - 1$ est premier lorsque n prend l'une des valeurs suivantes : 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1 279, 2 203, 2 281, 3 217, 4 253 et 4 423.
Le plus grand nombre de Mersenne premier connu depuis 1998 est $2^n - 1$, avec $n = 3\,021\,377$.

85 Nombres de Fermat

On appelle nombre de Fermat tout entier naturel F_n de la forme $F_n = 2^{2^n} + 1$, où n est un entier naturel.
1. *a)* Calculer F_0, F_1, F_2 et F_3.
Vérifier que ces nombres sont premiers.
b) Vérifier que F_5 est divisible par 641.
2. Démontrer que : $\forall\, n \in \mathbb{N}$, $F_{n+1} = (F_n - 1)^2 + 1$.
3. Démontrer par récurrence que pour tout entier naturel n strictement supérieur à 1, l'écriture décimale de F_n se termine par 7. *(On pourra utiliser les congruences.)*
4. Soit k un entier naturel non nul.
a) En posant $a = 2^{2^n}$, démontrer que :

$$\frac{F_{n+k} - 2}{F_n} = \frac{a^{2^k} - 1}{a + 1}.$$

b) En déduire que F_n divise $F_{n+k} - 2$.
5. Déduire de la question précédente que deux nombres de Fermat distincts sont premiers entre eux.

86 Des urnes et des billes

Trois urnes contiennent des billes. Chaque urne est suffisamment grande pour contenir la totalité des billes. La seule opération autorisée est de doubler le nombre de billes contenues dans une urne en prélevant des billes dans une autre.
Démontrer qu'il est possible, quel que soit la configuration initiale, d'obtenir une configuration où l'une des urnes est vide.