COURS MATHÉMATIQUES

Terminale S

Arithmétique

Table des matières

Table des matières **3**

I Arithmétique **5**
I.1 Les ensembles $\mathbb{N}$ et $\mathbb{Z}$ . . . 5
I.1.1 L'ensemble $\mathbb{N}$ . . . 5
I.1.2 L'ensemble $\mathbb{Z}$ . . . 6
I.1.3 Numération . . . 9
I.1.4 Exercices . . . 11
I.2 Multiples et diviseurs d'un entier relatif . . . 11
I.2.1 Multiples d'un entier relatif . . . 11
I.2.2 Diviseurs d'un entier relatif . . . 13
I.2.3 Ensemble des diviseurs d'un entier relatif . . . 13
I.2.4 Exercices résolus . . . 14
I.2.5 Exercices . . . 15
I.3 Nombres premiers . . . 15
I.3.1 Généralités . . . 15
I.3.2 Décomposition en produit de facteurs premiers . . . 17
I.4 PPCM et PGCD de deux entiers relatifs . . . 19
I.4.1 PPCM de deux entiers relatifs . . . 19
I.4.2 PGCD de deux entiers relatifs . . . 20
I.4.3 Déterminations du PGCD et du PPCM de deux entiers naturels . . . 22
I.4.4 Nombres premiers entre eux . . . 24
I.4.5 Équations diophantiennes . . . 26
I.4.6 Exercices . . . 27
I.5 Congruence modulo n . . . 28
I.5.1 Définition et propriétés immédiates . . . 28
I.5.2 Petit théorème de FERMAT . . . 30
I.5.3 Résolution d'équations avec congruences . . . 31
I.5.4 Utilisations des congruences . . . 35
I.5.5 Exercices . . . 41
I.6 Nombres premiers . . . 41
I.6.1 Généralités . . . 41
I.6.2 Décomposition en produit de facteurs premiers . . . 44

Index **46**

Chapitre I

Arithmétique

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 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.

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

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

$\mathbb{N}$ désigne l'ensemble des entiers naturels et $\mathbb{N}^\star$ désigne l'ensemble des entiers naturels non nuls. On a : $\mathbb{N} = \{0;1;2;3;\ldots;n;n+1;\ldots\}$ et $\mathbb{N}^\star = \mathbb{N} \setminus \{0\}$.

I.1.1.a 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 principales 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 +	
$a+b=0\Longrightarrow a=b=0$	$a\times b=1\Longrightarrow a=b=1$

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

I.1.1.b Ordre dans $\mathbb{N}$

On définit dans $\mathbb{N}$ une relation, notée $\leqslant$, par : $\forall(a;b)\in\mathbb{N}^2,(a\leqslant b\Leftrightarrow\exists c\in\mathbb{N},b=a+c)$.
Cette relation possède les propriétés suivantes, dont la démonstration est immédiate.

THÉORÈME I.1.1

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

(1)	$a \leqslant a$	La relation $\leqslant$ est réflexive.
(2)	si $(a \leqslant b)$ et $(b \leqslant a)$, alors $a = b$	La relation $\leqslant$ est antisymétrique.
(3)	si $(a \leqslant b)$ et $(b \leqslant c)$, alors $(a \leqslant c)$	La relation $\leqslant$ est transitive.

Remarques

1. Une relation binaire à la fois réflexive, antisymétrique et transitive est une relation d'ordre.

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

3. Une relation d'ordre partiel est une relation d'ordre non total. Par exemple $\subset$ sur $\mathscr{P}(\mathbb{N})$ est une relation d'ordre partiel.

On admet le théorème suivant.

THÉORÈME I.1.2

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

Exemples

1. Le plus petit élément de $\mathbb{N}$ est 0.

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

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

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

I.1.2.a Addition dans $\mathbb{Z}$

L'ensemble $\mathbb{Z}$ muni de l'addition possède les propriétés suivantes.

THÉORÈME I.1.3

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

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

Remarque Un entier relatif a n'admet qu'un seul opposé, on le note $(-a)$.

Vocabulaire Pour résumer ses propriétés, on dit que $(\mathbb{Z}, +)$ est un groupe.
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 cet ensemble admet un « symétrique » dans cet ensemble.

Remarque Soit $\mathscr{I}$ l'ensemble des isométries du plan. $(\mathscr{I}, \circ)$ est un groupe ; en effet :

- la composée de deux isométries est une isométrie ;
- la composée des isométries est associative ;
- l'application identique (élément neutre pour $\circ$) est une isométrie ;
- la réciproque d'une isométrie est une isométrie.

THÉORÈME I.1.4

Pour tous entiers relatifs a et b, on a : $a+b=b+a$. L'addition dans $\mathbb{Z}$ est commutative.

On dit que $(\mathbb{Z},+)$ est un groupe commutatif (ou abélien).

Remarques

1. $(\mathbb{R},+)$ et $(\mathbb{R}^\star,\times)$ sont des groupes commutatifs.

2. Le groupe $(\mathscr{S},\circ)$ est non commutatif.

THÉORÈME I.1.5

Pour tous entiers relatifs a, b et c on a :
si $a+b=a+c$, alors $b=c$.

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

I.1.2.b Multiplication dans $\mathbb{Z}$

L'ensemble $\mathbb{Z}$ muni de la multiplication possède les propriétés suivantes.

THÉORÈME I.1.6

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

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

$(\mathbb{Z},+)$ est un groupe commutatif ; de plus $\times$ est une loi de composition interne à $\mathbb{Z}$, associative, distributive par rapport à $+$ et présente un élément neutre, 1, on dit que $(\mathbb{Z},+,\times)$ est un anneau. De plus $\times$ est commutative dans $\mathbb{Z}$, on dit que $(\mathbb{Z},+,\times)$ est un anneau commutatif.

THÉORÈME I.1.7

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

(1) $b\times 0=0$;

(2) si $ab=0$ alors $a=0$ ou $b=0$.

Démonstration Nous ne démontrerons que la première propriété.

On a : $bb+b\times 0=b(b+0)=bb=bb+0$; donc : $b\times 0=0$. □

Remarques

1. Plus généralement un produit d'entier est nul si et seulement si l'un au moins des en tiers est nul.

2. On déduit de **(2)** que si $ab=ac$ et $a\neq 0$, alors $b=c$.

I.1.2.c 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 $\leqslant$, par : $\forall(a,b)\in\mathbb{Z}^2,\big(a\leqslant b\iff b-a\in\mathbb{N}\big)$.
Cette relation est une relation d'ordre total.

On admet les deux théorèmes suivants.

THÉORÈME I.1.8

Soit a et b deux entiers relatifs.

(1) Pour tout entier relatif c, on a : $a \leqslant b \iff a+c \leqslant b+c$.

(2) Pour tout entier naturel non nul c, on a : $a \leqslant b \iff ac \leqslant bc$.

Remarque Lorsqu'on multiplie chaque membre d'une inégalité par un nombre strictement négatif, l'inégalité change de sens.

THÉORÈME I.1.9

Toute partie bornée non vide de $\mathbb{Z}$ admet un plus petit et un plus grand élément.

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

THÉORÈME I.1.10

Soit a et b deux entiers relatifs tels que : $b \neq 0$.

Il existe un entier relatif n tel que : $nb \geqslant a$.

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

Démonstration 1er cas : $b \geqslant 1$

- Si $a \geqslant 0$, il suffit de prendre $n = a$.
- Si $a < 0$, il suffit de prendre $n = 0$.

2e cas : $b \leqslant -1$

On a : $-b \geqslant 1$; donc il existe un entier relatif m, tel que : $m(-b) \geqslant a$.

Il suffit donc de prendre : $n = -m$. □

I.1.2.d Division euclidienne dans $\mathbb{Z}$

THÉORÈME I.1.11

Soit a et b deux entiers relatifs tels que $b \neq 0$.

Il existe un unique couple (q, r) élément de $\mathbb{Z} \times \mathbb{N}$ tel que : $a = bq + r$ et $0 \leqslant r < |b|$.

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 reste et son quotient.

Démonstration

Existence

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

A n'est pas vide car $a + |ba|$ est élément de A.

A est une partie non vide de $\mathbb{N}$, donc A admet un plus petit élément r.

On a : $r \in$A et A$\subset \mathbb{N}$; donc : $0 \leqslant r$.

Il existe un entier relatif q tel que : $r = a - bq$.

On a : $r - |b| = a - bq - |b|$; donc il existe un entier relatif q' tel que : $r - |b| = a - bq'$.

r est le plus petit élément de A et : $r - |b| < r$; donc : $r - |b| \notin$A ; d'où : $r - |b| < 0$.

Il existe donc un couple (q, r) tel que : $a = bq + r$ et $0 \leqslant r < |b|$.

Unicité

Soit (q, r) et (q', r') deux couples tels que : $a = bq + r$; $a = bq' + r'$; $0 \leqslant r < |b|$ et $0 \leqslant r' < |b|$.

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

Or : $0 \leqslant r' < |b|$ et $-|b| < -r \leqslant 0$; donc : $-|b| < r' - r < |b|$; d'où : $|r' - r| < |b|$; c'est-à-dire : $|b|\,|q' - q| < |b|$.

De plus : $|b| \neq 0$; donc par quotient : $|q' - q| < 1$; d'où : $|q' - q| = 0$; c'est-à-dire : $q' = q$.

De plus : $r' = a - bq' = a - bq = r$; le couple (q, r) est donc unique. □

Pour démontrer qu'un objet U est l'unique objet vérifiant une propriété, il suffit de démontrer que tout objet U' vérifiant la propriété est égal à U.

Exemples

1. $a = 47$ et $b = 9$
On a : $47 = 9 \times 5 + 2$ et $0 \leqslant 2 < 9$.
Donc : $q = 5$ et $r = 2$.

2. $a = 47$ et $b = -9$
On a : $47 = (-9) \times (-5) + 2$ et $0 \leqslant 2 < 9$.
Donc : $q = -5$ et $r = 2$.

3. $a = -47$ et $b = 9$
On a : $-47 = 9 \times (-6) + 7$ et $0 \leqslant 7 < 9$.
Donc : $q = -6$ et $r = 7$.

4. $a = -53$ et $b = -12$
On a : $-53 = (-12) \times 5 + 7$ et $0 \leqslant 7 < 12$.
Donc : $q = 5$ et $r = 7$.

Remarque Lorsque b est positif, on peut effectuer la division euclidienne de a par b, à l'aide d'une calculatrice, en utilisant les formules : $q = \mathrm{E}\left(\frac{a}{b}\right)$ et $r = a - qb$, où E désigne la fonction partie entière.

Exemple Effectuer la division euclidienne de $-23\,564$ par $1\,229$.
On a : $\frac{-23\,564}{1\,229} = -19,1\ldots$; donc : $q = \mathrm{E}\left(\frac{-23\,564}{1\,229}\right) = -20$ et $r = -23\,564 - 1\,229 \times (-20) = 1\,016$.

I.1.3 Numération

I.1.3.a Bases de numération

L'homme compte depuis l'aube de l'humanité. Il commença par compter sur ses dix doigts, aujourd'hui il utilise le système décimal, ou base dix. Ainsi le nombre que nous désignons par 51 253 est, d'après notre système usuel de numération : $5 \times 10^4 + 1 \times 10^3 + 2 \times 10^2 + 5 \times 10^1 + 3 \times 10^0$.

La base dix s'est imposée par l'usage. Les ordinateurs comptent en base deux (système binaire) ; les gens qui programment les ordinateurs en assembleur utilisent des codes en base 16 (système hexadécimal) ; les navigateurs expriment la latitude et la longitude en degrés, minutes et secondes ; ils comptent donc en base soixante (système sexagésimal).

On admet le théorème suivant.

THÉORÈME I.1.12

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

La suite $a_0, a_1, \ldots, a_n$ est appelée développement de x en base p et l'on écrit : $x = \overline{a_n a_{n-1} \ldots a_1 a_0}^{p}$.

Remarque Le quotient et le reste de la division euclidienne de x par p sont respectivement : $q_0 = \overline{a_n a_{n-1} \ldots a_1}^{p}$ et a_0.
Le quotient et le reste de la division euclidienne de q_0 par p sont respectivement : $q_1 = \overline{a_n a_{n-1} \ldots a_2}^{p}$ et a_1.
On peut ainsi déterminer de proche en proche tous les chiffres de l'entier naturel x écrit en base p.

Exemples

1. On a : $121 = 4 \times 5^2 + 4 \times 5^1 + 1 \times 5^0$; donc : $121 = \overline{441}^{5}$.

2. Pour convertir 134 en base 7, on effectue des divisions successives par 7 en commençant par 134, comme indiqué sur la figure ci-contre.
On en déduit que : $134 = \overline{251}^{7}$.

134	7			
1	19	7		
	5	2	7	
		2	0	

I.1.3.b Système binaire

Pour écrire un nombre en base 2, l'ensemble des chiffres utilisé est : $\{0;1\}$.

Exercice I.1.1. ***Convertir en base dix le nombre : $\overline{10010011101}^{2}$.***

Solution *On a :* $\overline{10010011101}^{2} = 2^{10}+2^{7}+2^{4}+2^{3}+2^{2}+2^{0}$ □
$= 1024+128+16+8+4+1$
$= 1181$

Exercice I.1.2. ***Convertir en base deux le nombre : 203.***

Solution *Effectuons des divisions successives par 2 en commençant par 203, comme indiqué sur la figure ci-dessous.*

203	2							
1	101	2						
	1	50	2					
		0	25	2				
			1	12	2			
				0	6	2		
					0	3	2	
						1	1	2
							1	0

On en déduit que : $203 = \overline{11001011}^{2}$. □

I.1.3.c Système hexadécimal

Pour écrire un nombre en base 16, l'ensemble des chiffres utilisé est :

$$\{0;1;2;3;4;5;6;7;8;9;A;B;C;D;E;F\}$$

Les chiffres A, B, C, D, E et F représentent respectivement les nombres 10 ; 11 ; 12 ; 13 ; 14 et 15.

Exercice I.1.3. ***Convertir en base dix le nombre : $\overline{BAC}^{16}$.***

Solution *On a :* $\overline{BAC}^{16} = 11\times16^{2}+10\times16^{1}+12\times16^{0}$ □
$= 2816+160+12$
$= 2988$

Exercice I.1.4. ***Convertir en base seize le nombre : 51 966.***

Solution *Effectuons des divisions successives par* 16 *en commençant par* 51 966*, comme indiqué sur la figure ci-contre.*
On en déduit que : $51966 = \overline{CAFE}^{16}$.

51966	16			
14	3247	16		
	15	202	16	
		10	12	16
			12	0

□

I.1.4 Exercices

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

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

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

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

I.1.d. Démontrer par récurrence que pour tout entier naturel n supérieur ou égal à 3, on a : $n! \geqslant 2^{n-1}$.

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

- $a = 61$ et $b = 17$
- $a = 61$ et $b = -17$
- $a = -61$ et $b = 17$
- $a = -61$ et $b = -17$
- $a = 6327$ et $b = 628$

I.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.

I.1.g. Écrire en base 2 les nombres : 19 ; 157 et 987.

I.1.h. Écrire en base 10 les nombres : $\overline{10110}^2$; $\overline{11011}^2$ et $\overline{101011}^2$.

I.1.i. Écrire en base 16 les nombres : 19 ; 157 et 987.

I.1.j. Écrire en base 10 les nombres : $\overline{16}^{16}$; $\overline{1A}^{16}$ et $\overline{2A}^{16}$.

I.1.k. Écrire en base 6 le nombre : $\overline{1234}^5$.

I.1.l. Déterminer les couples de chiffres $(x;y)$ tels que le nombre d'écriture décimale $\overline{724xy}$ soit multiple de 9.

I.2 Multiples et diviseurs d'un entier relatif

I.2.1 Multiples d'un entier relatif

I.2.1.a Définition et propriétés

DÉFINITION I.2.1

Soit a et b deux entiers relatifs.

a est un *multiple* de b s'il existe un entier relatif k tel que : $a = kb$.

Exemples

1. On a : $99 = 9 \times 11$ et $11 \in \mathbb{Z}$; donc 99 est multiple de 9 (et de 11).

2. $-21, -14, -7, 0, 7, 14, 21$ sont des multiples de 7 et de -7.

Remarques

1. Tout entier relatif est multiple de -1 et de 1.

2. 0 est multiple de tout entier relatif.

THÉORÈME I.2.1

Soit a et b deux entiers relatifs tels que b est non nul.

a est multiple de b si et seulement si le reste de la division euclidienne de a par b est 0.

Démonstration Soit q le quotient et r le reste de la division euclidienne de a par b. On a : $a = bq + r$, avec $0 \leqslant r < |b|$.

Si $r = 0$, alors : $a = bq + 0$; donc a est multiple de b.

Réciproquement, si a est multiple de b, il existe un entier relatif k tel que : $a = bk = bk + 0$.

On peut donc prendre $q = k$ et $r = 0$ or d'après le théorème I.1.11 le couple $(q;r)$ est unique, donc : $r = 0$. □

THÉORÈME I.2.2

Soit a et b deux entiers relatifs.

Si a est multiple de b et si $a \neq 0$ alors : $|a| \geqslant |b|$.

Démonstration Soit a et b deux entiers relatifs tels que a est multiple de b et $a \neq 0$.

Il existe un entier k tel que $a = kb$; donc : $|a| = |k|\,|b|$.

De plus : $a \neq 0$; donc : $|k| \neq 0$; d'où : $|k| \geqslant 1$.

En multipliant cette dernière inégalité membre à membre par $|b|$, il vient : $|a| \geqslant |b|$. □

THÉORÈME I.2.3

Soit a, b et c trois entiers relatifs.

(1) a est multiple de a.

(2) Si a est multiple de b et b est multiple de a, alors $a = b$ ou $a = -b$.

(3) Si a est multiple de b et b est multiple de c, alors a est multiple de c.

Démonstration

(1) $a = 1 \times a$ donc a est multiple de a.

(2) Si a est multiple de b et b est multiple de a, alors d'après le théorème I.2.2 : $|a| \geqslant |b|$ et $|a| \leqslant |b|$; d'où : $|a| = |b|$; c'est-à-dire : $a = b$ ou $a = -b$.

(3) Si a est multiple de b et b est multiple de c, alors : $a = kb$ $(k \in \mathbb{Z})$ et $b = k'c$ $(k' \in \mathbb{Z})$; donc : $a = (kk')c$ $(kk' \in \mathbb{Z})$. Ce qui signifie que a est multiple de c. □

Remarque Dans $\mathbb{N}$, la relation « est multiple de » est une relation d'ordre partiel.

THÉORÈME I.2.4

Soit a, b et n trois entiers relatifs.

Si a et b sont multiples de n alors, pour tous entiers u et v, $au + bv$ est multiple de n.

Démonstration On a : $a = a'n$ et $b = b'n$ (avec $a' \in \mathbb{Z}$ et $b' \in \mathbb{Z}$) ; donc : $au + bv = (\underbrace{a'u + b'v}_{\in\mathbb{Z}})n$. □

Exemples

1. L'opposé d'un entier relatif pair est un entier relatif pair.

2. La somme de deux entiers relatifs pairs est un entier relatif pair.

I.2.1.b Ensemble des multiples d'un entier relatif

Soit n un entier relatif. Les multiples de n sont les nombres :

$$\cdots,\ n \times (-2),\ n \times (-1),\ n \times (0),\ n \times (1),\ n \times (2),\ \cdots$$

ces nombres sont de la forme : nk , où $k \in \mathbb{Z}$.

Notation

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

Exemples

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

2. $1\mathbb{Z} = \mathbb{Z}$

3. $0\mathbb{Z} = \{0\}$

Remarques

1. Pour tout entier n : $n\mathbb{Z} = (-n)\mathbb{Z}$; donc, en pratique, on utilise cette notation lorsque n est un entier naturel.

2. Pour tout entier naturel n, $(n\mathbb{Z}, +)$ est un groupe commutatif.

I.2.2 Diviseurs d'un entier relatif

DÉFINITION I.2.2

Soit a et b deux entiers relatifs.
b est un *diviseur* de a (ou b divise a) si a est multiple de b.

Exemples

1. -4 divise 12 car : $12 = -4 \times (-3)$ et $-3 \in \mathbb{Z}$.
2. 9 divise 234 car : $234 = 9 \times 26$ et $26 \in \mathbb{Z}$.
3. 32 divise 323232 car : $323232 = 32 \times 10101$ et $10101 \in \mathbb{Z}$.

Remarques

1. -1 et 1 divisent tout entier relatif.
2. Pour tout entier n, n et $-n$ sont des diviseurs de n.

Notations et vocabulaire Les diviseurs d'un entier n autre que : $-n$; -1 ; 1 et n ; sont appelés *diviseurs propres* de n. Par exemple 2 et 6 sont des propres de 12.

Les théorèmes suivant ne sont que des reformulations des théorèmes I.2.1, I.2.2, I.2.3, I.2.4 page 11 établis au paragraphe I.2.1.a.

THÉORÈME I.2.5

Soit a et b deux entiers relatifs tels que b est non nul.
b divise a si et seulement si le reste de la division euclidienne de a par b est 0.

THÉORÈME I.2.6

Soit a et b deux entiers relatifs tels que a est non nul.
Si b divise a, alors : $|b| \leqslant |a|$.

THÉORÈME I.2.7

Soit a, b et c trois entiers relatifs.
(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.

Remarque Dans $\mathbb{N}$, la relation « divise » est une relation d'ordre partiel.

THÉORÈME I.2.8

Soit a, b et c trois entiers relatifs.
(1) Si a divise b, alors $-a$ divise b.
(2) Si c divise a et b alors, pour tous entiers u et v, c divise $au + bv$.

I.2.3 Ensemble des diviseurs d'un entier relatif

Notation

Soit a et b deux entiers relatifs.
$\mathscr{D}(a)$ désigne l'ensemble des diviseurs de a.
$\mathscr{D}(a;b)$ désigne l'ensemble des diviseurs communs à a et b.

Exemples

1. $\mathscr{D}(1) = \{-1;1\}$
2. $\mathscr{D}(4) = \{-4;-2;-1;1;2;4\}$
3. $\mathscr{D}(6) = \{-6;-3;-2;-1;1;2;3;6\}$
4. $\mathscr{D}(4;6) = \{-2;-1;1;2\}$

Remarques

1. $\mathscr{D}(a;b) = \mathscr{D}(a) \cap \mathscr{D}(b)$.

2. Si $a \neq 0$, $\mathscr{D}(a)$ est un ensemble borné non vide ($1 \in \mathscr{D}(a)$ et $\forall d \in \mathscr{D}(a)$, $|d| \leqslant |a|$).

3. Si a et b ne sont pas tous nuls, $\mathscr{D}(a;b)$ est de même borné et non vide ($1 \in \mathscr{D}(a;b)$ et $\forall d \in \mathscr{D}(a;b)$, $|d| \leqslant |a|$ ou $|d| \leqslant |b|$).

THÉORÈME I.2.9

Soit a, b et q trois entiers relatifs.
On a : $\mathscr{D}(a;b) = \mathscr{D}\big(b;a-bq\big)$.

Démonstration Soit c un élément de $\mathscr{D}(a;b)$.
Il existe deux entiers relatifs k et k' tels que : $a = kc$ et $b = k'c$.
On a : $a - bq = (k - k'q)c$; donc : $c \in \mathscr{D}\big(b;a-bq\big)$.
Par conséquent : $\mathscr{D}(a;b) \subset \mathscr{D}\big(b;a-bq\big)$.
Soit c un élément de $\mathscr{D}\big(b;a-bq\big)$.
Il existe deux entiers relatifs k et k' tels que : $b = kc$ et $a - bq = k'c$.
On a : $a = a - bq + bq = k'c - kcq = (k' - kq)c$; donc : $c \in \mathscr{D}(a;b)$.
Par conséquent : $\mathscr{D}\big(b;a-bq\big) \subset \mathscr{D}(a;b)$.
On a : $\mathscr{D}(a;b) \subset \mathscr{D}\big(b;a-bq\big)$ et $\mathscr{D}\big(b;a-bq\big) \subset \mathscr{D}(a;b)$; donc : $\mathscr{D}(a;b) = \mathscr{D}\big(b;a-bq\big)$. □

Pour démontrer l'égalité de deux ensembles E et E', on peut établir leur double inclusion ; c'est-à-dire démontrer que : $E \subset E'$ et $E' \subset E$.

I.2.4 Exercices résolus

Exercice I.2.1. ***Résoudre dans $\mathbb{N}^2$ l'équation :***

$$x^2 - y^2 = 35 \tag{I.1}$$

Solution

$$(I.1) \iff (x-y)(x+y) = 35$$

Soit $(x;y)$ un couple d'entiers naturels solution de l'équation (I.1) (s'il en existe).
Raisonnons par conditions nécessaires.
D'après l'équivalence ci-dessus, $(x-y)$ et $(x+y)$ sont des diviseurs « conjugués » de 35.
y est positif, donc : $x - y \leqslant x + y$. De plus $(x+y)$ est positif, donc $(x-y)(x+y)$ est du signe de $(x-y)$ or ce produit est positif, donc $(x-y)$ est positif, c'est-à-dire : $y \leqslant x$.
L'ensemble des diviseurs naturels de 35 est :

$$\mathscr{D}(35) = \{1;5;7;35\}.$$

En remarquant que : $x = \dfrac{(x+y)+(x-y)}{2}$ et $y = \dfrac{(x+y)-(x-y)}{2}$, on en déduit le tableau suivant qui donne à la fois toutes les solutions potentielles et leur vérification.

$x-y$	$x+y$	x	y	x^2-y^2
1	35	18	17	$18^2 - 17^2 = 324 - 289 = 35$
5	7	6	1	$6^2 - 1^2 = 36 - 1 = 35$

$$S = \{(6;1),(18;17)\}$$

□

I.2.5 Exercices

I.2.a. Combien y a-t-il de multiples de 11 compris entre −1000 et 1000 ?

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

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

I.3 Nombres premiers

I.3.1 Généralités

I.3.1.a Définition et propriété

Lorsqu'un entier naturel non nul admet un diviseur propre, on dit qu'il est *composé* car on peut le décomposer. Par exemple, 2 est un diviseur propre de 6 et on a la décomposition : $6 = 2 \times 3$. Dans une décomposition, par exemple : $1860 = 10 \times 6 \times 31$, il peut arriver que certains facteurs soit composés ; on peut alors désirer pousser la décomposition au maximum. Dans l'exemple précédent on obtient : $1860 = 2^2 \times 3 \times 5 \times 31$. On constate qu'on a utiliser les nombres 2 ; 3 ; 5 et 31 pour décomposer 1860. Plus généralement les entiers qui servent à décomposer complètement les entiers naturels supérieurs strictement à 1 sont appelés *nombres premiers*.

DÉFINITION I.3.1

Un *nombre premier* p est un entier naturel qui possède exactement deux diviseurs positifs : 1 et p.

Exemples

1. Les six premiers nombres premiers sont : 2 ; 3 ; 5 ; 7 ; 11 ; 13.

2. 6 et 121 ne sont pas des nombres premiers car : $6 = 2 \times 3$ et $121 = 11 \times 11$.

Remarques

1. 0 et 1 ne sont pas des nombres premiers.

2. Deux nombres premiers distincts sont premiers entre eux (car 1 est le diviseur commun positif).

THÉORÈME I.3.1

Tout entier naturel $n \geqslant 2$ admet au moins un diviseur premier.

Démonstration Soit A l'ensemble des diviseurs de n supérieurs ou égaux à 2 : $A = \{d \geqslant 2 \mid d \in \mathscr{D}(n)\}$.
On a : $n \in A$; donc A n'est pas vide, par conséquent il admet un plus petit élément p.
Si p était composé il admettrait un diviseur propre positif p' qui serait à la fois élément de A et strictement plus petit que le plus petit élément de A, ce qui est contradictoire ; donc p est un nombre premier et puisque $p \in A$, p est un diviseur de n. □

Remarque L'ensemble des diviseurs premiers de n n'est pas vide, il admet donc un plus petit élément : le plus petit diviseur premier de n.

I.3.1.b Ensemble des nombres premiers

THÉORÈME I.3.2

Il existe une infinité de nombres premiers

DémonstrationSi l'ensemble des nombres premiers était fini il aurait un plus grand élément $p^{\sim}$, $p^{\sim}!$ serait alors

mul-

tiple de tous les nombres premiers et $\tilde{p}!+1$ n'aurait donc aucun diviseur premier, ce qui est en contradiction avec le théorème I.6.1. Il existe donc une infinité de nombres premiers □

I.3.1.c Comment savoir si un nombre est premier

Un premier algorithme

THÉORÈME I.3.3

Soit n un entier naturel($n \geqslant 2$).
Si n n'est pas premier alors il admet au moins un diviseur d tel que : $2 \leqslant d^2 \leqslant n$.

DémonstrationSi n n'est pas premier, il admet au moins un diviseur entier naturel autre que 1 et n. Il existe donc deux entiers naturels d et d' tels que : $n = d \times d'$ et $2 \leqslant d \leqslant d'$. On a donc : $2 \leqslant d$; et en multipliant la seconde inégalité membre à membre par d on obtient : $d^2 \leqslant n$. □

Remarques

1. D'après le théorème I.6.1, d admet un diviseur premier p et on a donc : $p^2 \leqslant n$; c'est-à-dire : $p \leqslant \sqrt{n}$.

2. En pratique c'est la contraposée de cette dernière implication qui est utilisée : « si n n'a aucun diviseur premier, p, tel que : $p \leqslant \sqrt{n}$; alors n est premier ».

Exercice I.3.1. **163 *est-il un nombre premier ?***

Solution *On a :* $\sqrt{163} = 12,7\cdots$ *; les nombres premiers p vérifiant :* $p \leqslant \sqrt{163}$ *; sont :* 2 ; 3 ; 5 ; 7 *et* 11.

On a : $163 = 2 \times 81 + 1$ *et* $0 < 1 < 2$ *: donc* 163 *n'est pas multiple de* 2.
$163 = 3 \times 54 + 1$ *et* $0 < 1 < 3$ *: donc* 163 *n'est pas multiple de* 3.
$163 = 5 \times 32 + 3$ *et* $0 < 3 < 5$ *: donc* 163 *n'est pas multiple de* 5.
$163 = 7 \times 23 + 2$ *et* $0 < 2 < 7$ *: donc* 163 *n'est pas multiple de* 7.
$163 = 11 \times 14 + 9$ *et* $0 < 9 < 11$ *: donc* 163 *n'est pas multiple de* 11.

163 *n'est divisible par aucun des nombres premiers p vérifiant :* $p \leqslant \sqrt{163}$ *; donc* 163 *est un nombre premier.*□

Le crible d'Ératostène

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 ; dans les tableaux I.3 et I.4, on a : $n = 127$.

- On représente dans un tableau les entiers naturels successifs compris entre 2 et n.
- Le nombre 2 est premier. On barre tous les multiples de 2 autre que 2.
- **Exemple** 6 est diviseur de 54 car $54 = 6 \times 9$.

  Le premier nombre non barré est 3, qui est donc premier. On barre tous les multiples de 3 autre que 3.
- On itère le procédé jusqu'à ce qu'il ne reste plus de nombre composé.

À partir des multiples de quel nombre premier est-on sûr d'avoir barré tous les nombres composés ?

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
101	102	103	104	105	106	107	108	109
110	111	112	113	114	115	116	117	118
119	120	121	122	123	124	125	126	127

TAB. I.1 – Crible d'ÉRATOSTHÈNE (début)

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~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109
~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~
~~119~~	~~120~~	~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127

TAB. I.2 – Crible d'ÉRATOSTHÈNE (fin)

I.3.1.d Nombres premiers et divisibilité

THÉORÈME I.3.4

Soit p un nombre premier et a un entier relatif.
Si a n'est pas divisible par p alors a et p sont premiers entre eux.

Démonstration Les diviseurs naturels de p sont 1 et p, donc si p n'est pas un diviseur de a alors leur seul diviseur naturel commun est 1 ; d'où : $\text{PGCD}(a;p) = 1$. □

Remarque En particulier deux nombres premiers distincts sont premiers entre eux.

THÉORÈME I.3.5

Soit p un nombre premier et a, b deux entiers relatifs.
(1) Si p divise ab alors p divise a ou p divise b.
(2) Si de plus a et b sont premiers alors $p = a$ ou $p = b$.

Démonstration **(1)** Si p divise a, alors le résultat est acquis ; sinon p divise ab et, d'après le théorème I.6.4, p est premier avec a donc, d'après le théorème de GAUSS, p divise b.
(2) Si de plus a et b sont premiers alors les diviseurs naturels de a sont 1 et a et ceux de b sont 1 et b, comme $p \neq 1$ on en déduit que : $p = a$ ou $p = b$. □

Plus généralement ce théorème s'étend, par récurrence, à un nombre quelconque de facteurs et nous obtenons alors le corollaire suivant que nous admettons.

COROLLAIRE I.3.6

Soit p un nombre premier et $a_1, a_2, \cdots, a_n$, n entiers relatifs (avec $n \geqslant 2$).
(1) Si p divise $a_1 \times a_2 \times \cdots \times a_n$ alors p divise l'un des facteurs a_i.
(2) Si de plus les facteurs a_i sont premiers alors p est l'un d'eux.

Remarque En particulier si p divise a^n (avec $n \leqslant 1$) alors p divise a.

I.3.2 Décomposition en produit de facteurs premiers

I.3.2.a Théorème fondamental de l'arithmétique

On a vu en introduction des nombres premiers que les nombres premiers peuvent servir à décomposer les autres entiers naturels en produit, par exemple :

- on a : $12 = 2^2 \times 3$;
- on a : $3 = 3$ (3 est un nombre premier) ;
- on a : $720 = 2^4 \times 3^2 \times 5$.

Plus généralement, on a le théorème suivant.

THÉORÈME I.3.7 THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE

Soit a un entier tel que : $a \geqslant 2$.
Il existe un entier naturel non nul n, n nombres premiers distincts $p_1, \ldots, p_n$ et n entiers naturels tous non nuls $\alpha_1, \cdots, \alpha_n$ tels que :

$$a = p_1^{\alpha_1} \times \cdots \times p_n^{\alpha_n} \qquad \text{et} \qquad p_1 < p_2 < \cdots < p_n.$$

De plus cette décomposition est unique.

Démonstration

Existence

Considérons pour tout entier $a \geqslant 2$ la proposition P_a : « pour tout entier b tel que : $2 \leqslant b \leqslant a$; Il existe un entier naturel non nul n, n nombres premiers distincts $p_1, \cdots, p_n$ et n entiers naturels tous non nuls $\alpha_1, \cdots, \alpha_n$ tels que : $b = p_1^{\alpha_1} \times \cdots \times p_n^{\alpha_n}$ et $p_1 < p_2 < \cdots < p_n$ ».
Pour $a = 2$, on a : $b = 2$; $n = 1$; $p_1 = 2$ et $\alpha_1 = 1$ car $2 = 2^1$. Donc P_2 est vraie.
Soit a un entier naturel supérieur ou égal à 2 pour lequel P_a est vraie ; démontrons P_{a+1}.
Il suffit de déterminer une décomposition de $a+1$ en produit de facteurs premiers. Deux cas sont envisageables.

1er cas : $a+1$ est premier Alors : $a+1 = (a+1)^1$; on a donc : $n = 1$; $p_1 = a+1$; $\alpha_1 = 1$ et P_{a+1} est acquise.

2e cas : $a+1$ n'est pas premier Soit p le plus petit diviseur premier de $a+1$ (il existe d'après la remarque suivant le théorème I.6.1) et b le quotient de $a+1$ par p, on a donc : $a+1 = pb$.
$a+1$ n'est pas premier, donc : $2 \leqslant b \leqslant a$; d"après P_a, il existe donc un entier naturel non nul n, n nombres premiers distincts $p_1, \cdots, p_n$ et n entiers naturels tous non nuls $\alpha_1, \cdots, \alpha_n$ tels que : $b = p_1^{\alpha_1} \times \cdots \times p_n^{\alpha_n}$ et $p_1 < p_2 < \cdots < p_n$.
$p_1, \cdots, p_n$ sont des diviseurs premiers de b donc de $a+1$; d'où : $p \leqslant p_1$.
- Si $p < p_1$, alors $a+1 = p \times p_1^{\alpha_1} \times \cdots \times p_n^{\alpha_n}$ et $p < p_1 < p_2 < \cdots < p_n$;
- si $p = p_1$, alors $a+1 = p_1^{\alpha_1+1} \times p_2^{\alpha_2} \times \cdots \times p_n^{\alpha_n}$ et $p < p_1 < p_2 < \cdots < p_n$;

et P_{a+1} est également acquise.

Par récurrence on en déduit l'existence de la décomposition pour tout entier $a \geqslant 2$.

Unicité

Soit a un entier avec $a \geqslant 2$ et $a = p_1^{\alpha_1} \times \cdots \times p_n^{\alpha_n}$, $a = q_1^{\beta_1} \times \cdots \times q_n^{\beta_n}$ avec $p_1 < p_2 < \cdots < p_n$ et $q_1 < q_2 < \cdots < q_n$ deux décompositions en produits de facteurs premiers.
Démontrons que $m = n$ et que pour tout entier i compris entre 1 et n : $p_i = q_i$ et $\alpha_i = \beta_i$.
Soit i un entier compris entre 1 et n. p_i divise a donc p_i divise $q_1^{\beta_1} \times \cdots \times q_n^{\beta_n}$. On en déduit, d'après le corollaire I.6.6, que : $p_i \in \{q_1, \cdots, q_n\}$.
Pour tout entier i compris entre 1 et n on a : $p_i \in \{q_1, \cdots, q_n\}$; donc : $\{p_1, \cdots, p_n\} \subset \{q_1, \cdots, q_n\}$.
De même : $\{q_1, \cdots, q_n\} \subset \{p_1, \cdots, p_n\}$; donc : $\{p_1, \cdots, p_n\} = \{q_1, \cdots, q_n\}$.
On en déduit que $m = n$ puis par récurrence que : $p_1 = q_1$; $p_2 = q_2$; … ; $p_n = q_n$.
Il ne reste plus qu'à démontrer que pour tout entier i compris entre 1 et n : $\alpha_i = \beta_i$.
Soit i un entier compris entre 1 et n. $p_i^{\alpha_i}$ divise $p_1^{\beta_1} \times \cdots \times p_{i-1}^{\beta_{i-1}} \times p_i^{\beta_i} \times p_{i+1}^{\beta_{i+1}} \times \cdots \times p_n^{\beta_n}$ et (d'après les remarques consécutives au théorème I.6.4 et au corollaire I.4.11) est premier avec $p_1^{\beta_1} \times \cdots \times p_{i-1}^{\beta_{i-1}} \times p_{i+1}^{\beta_{i+1}} \times \cdots \times p_n^{\beta_n}$ donc, d'après le théorème de GAUSS : $p_i^{\alpha_i}$ divise $p_i^{\beta_i}$.

De même : $p_i^{\beta_i}$ divise $p_i^{\alpha_i}$; donc : $p_i^{\alpha_i} = p_i^{\beta_i}$; d'où : $\alpha_i = \beta_i$. □

I.3.2.b Nombres de diviseurs naturels d'un entier

Exercice I.3.2. ***Déterminer l'ensemble des diviseurs naturels de 224***

Solution *Décomposons 224 en produit de facteurs premiers. Il vient :*

$$224 = 2^5 \times 7.$$

Les diviseurs naturels de 224 sont donc les nombres, d, qui peuvent s'écrire sous la forme : $d = 2^\alpha \times 7^\beta$ avec $\alpha \in \{0;1;2;3;4;5\}$ et $\alpha \in \{0;1\}$.
On en déduit que 224 a 10 diviseurs naturels dont l'ensemble est :

$$\mathscr{D}(224) = \{1;2;4;8;16;32;7;14;28;56;112;224\}.$$

□

I.4 PPCM et PGCD de deux entiers relatifs

I.4.1 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 $a\mathbb{Z} \cap b\mathbb{Z}$ (on a donc : $A = a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^\star$). A est une partie non vide de $\mathbb{N}$ (car $|ab| \in A$), donc A admet un plus petit élément.

DÉFINITION I.4.1

Soit a et b deux entiers relatifs non nuls.
Le plus petit commun multiple de a et b, noté PPCM(a,b), est le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$.

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

Exercice I.4.1. ***Déterminer le PPCM de 8 et 3.***

Solution *Les premiers multiples strictement positifs de 8 sont : 8 ; 16 ; 24 ; ...*
le premier d'entre eux qui est multiple de 3 est 24 ; donc : PPCM$(3;8) = 24$. □

Remarques

1. 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 toujours se ramener à la recherche du PPCM de deux entiers naturels non nuls.
2. Pour tous entiers naturels non nuls a et b, on a : $\max\{a;b\} \leqslant$ PPCM$(a;b) \leqslant ab$.
3. Pour tous entiers naturels non nuls a et b, on a : PPCM$(a;b) = a \iff a \in b\mathbb{Z}$.

THÉORÈME I.4.1

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, par transitivité, 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 μq 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 $0 \leqslant r < \mu$; 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 : $a\mathbb{Z}\cap b\mathbb{Z} = \mu\mathbb{Z}$. □

Remarque Cette propriété signifie qu'un entier c est multiple de a et de b si et seulement si il est multiple de μ.

Exemple On sait que : PPCM (12 ; 16) = 48 ; donc un nombre est multiple de 12 et de 16 si et seulement si il est multiple de 48.

Exercice I.4.2. ***1. Déterminer le* PPCM *de 2 et 3.***

2. Soit n un entier relatif, démontrer que $n^3 - n$ est multiple de 6.

Solution ***1.*** *Les multiples strictement positifs de* 3 *sont :* 3 ; 6 ; … ; *parmi eux le plus petit entier pair est* 6, *donc :* PPCM (2 ; 3) = 6.

2. *On a :* $n^3 - n = n(n^2-1) = (n-1)\times n\times(n+1)$; $n^3 - n$ *est donc le produit de trois entiers consécutifs, l'un d'entre eux est multiple de* 3, *donc* $n^3 - n$ *est multiple de* 3.

$n\times(n+1)$ *est le produit de deux entiers consécutifs, l'un d'eux est multiple de* 2, *donc* $n^3 - n$ *est multiple de* 2.

$n^3 - n$ *est multiple de* 2 *et de* 3, *il est donc multiple de leur* PPCM, *c'est-à-dire de* 6. □

THÉORÈME I.4.2 (MULTIPLICATIVITÉ DU PPCM)

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

Démonstration Posons : μ = PPCM $(a ; b)$ et μ_1 = PPCM $(ka ; kb)$.

μ est multiple de a et b, il existe donc 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 : $k\mu$ est multiple de μ_1.

μ_1 est multiple de ka et kb, 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'' est multiple de μ. On en déduit que : μ_1 est multiple de $k\mu$.

μ_1 et $k\mu$ sont deux entiers *naturels* multiples l'un de l'autre, ils sont donc égaux. On a donc : PPCM $(ka ; kb) = k$ PPCM $(a ; b)$. □

Exercice I.4.3. ***Déterminer le PPCM de 45 et 120***

Solution *On a :* PPCM (45 ; 120) = PPCM (15 × 3 ; 15 × 8) = 15 × PPCM (3 ; 8).
Or on a vu que : PPCM (3 ; 8) = 24 *; donc :* PPCM (45 ; 120) = 15 × 24 = 360. □

I.4.2 PGCD de deux entiers relatifs

I.4.2.a Définition et propriétés

Soit a et b deux entiers relatifs non tous nuls. On a vu (remarque 3 §I.2.3 page 13) que l'ensemble $\mathscr{D}(a ; b)$ des diviseurs communs à a et b est non vide et borné, $\mathscr{D}(a ; b)$ admet donc un plus grand élément.

DÉFINITION I.4.2

Soit a et b deux entiers relatifs non tous nuls.
Le plus grand commun diviseur de a et b, noté PGCD $(a ; b)$, est le plus grand élément de $\mathscr{D}(a ; b)$.

Exemples

1. On a : $\mathscr{D}(12) = \{-12;-6;-4;-3;-2;-1;1;2;3;4;6;12\}$
$\mathscr{D}(15) = \{-15;-5;-3;-1;1;3;5;15\}$
$\mathscr{D}(12;15) = \{-3;-1;1;3\}$
Donc : PGCD $(12;15) = 3$.

2. $\mathscr{D}(7) = \{-7;-1;1;7\}$
Donc le PGCD de 7 et 24 est 7 ou 1 ; mais 7 ne divise pas 24 ; donc : PGCD $(7;24) = 1$.

Remarques

1. 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 toujours se ramener à la recherche du PGCD de deux entiers naturels non nuls.

2. Pour tous entiers naturels non nuls a et b, on a : $1 \leqslant$ PGCD $(a;b) \leqslant \min\{a;b\}$.

3. Pour tous entiers naturels non nuls a et b, on a : PGCD $(a;b) = b \iff b \in \mathscr{D}(a)$.

4. Pour tout entier naturel non nul c, on a : PGCD $(c;0) = c$.

THÉORÈME I.4.3

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

Démonstration

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

Soit d un élément de $\mathscr{D}(a;b)$. Désignons par μ le PPCM de d et δ ; on a donc : $\delta \leqslant \mu$.
a est multiple de d et de δ, donc a est multiple de μ. De même b est multiple de μ. Donc μ est un élément de $\mathscr{D}(a;b)$; donc : $\mu \leqslant \delta$; puis : $\mu = \delta$.
On a : PPCM $(d;\delta) = \delta$; donc d divise δ ; c'est-à-dire : $d \in \mathscr{D}(\delta)$. Donc : $\mathscr{D}(a;b) \subset \mathscr{D}(\delta)$.
On en déduit que : $\mathscr{D}(a;b) = \mathscr{D}(\delta)$. □

Remarque Ce théorème signifie qu'un entier d divise a et b si et seulement si il divise δ.

THÉORÈME I.4.4 (MULTIPLICATIVITÉ DU PGCD)

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 :

$$\delta_1 = qk\delta. \tag{I.2}$$

Il existe deux entiers naturels non nuls a'' et b'' tels que : $ka = \delta_1 a''$ et $kb = \delta_1 b''$.
D'après (I.2), on a donc : $ka = qk\delta a''$ et $kb = qk\delta b''$; or k n'est pas nul, donc : $a = q\delta a''$ et $b = q\delta b''$;
$q\delta$ divise a et b, donc $q\delta$ divise δ ; $q\delta$ et δ sont deux entiers *naturels* multiples l'un de l'autre, ils sont donc égaux.
En remplaçant $q\delta$ par δ dans (I.2), on obtient : $\delta_1 = k\delta$. □

Exercice I.4.4. ***Déterminer le PGCD de 300 et 375.***

Solution *On a :* PGCD $(300;375)$ = PGCD $(25\times12;25\times15) = 25\times$PGCD $(12;15)$ *;*
On a vu que : PGCD $(12;15) = 3$ *; donc :* PGCD $(300;375) = 25\times3 = 75$ □

THÉORÈME I.4.5

Soit a et b deux entiers relatifs non tous nuls et δ leur PGCD.
Les nombres de la forme : $au + bv$ (avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$) ; sont les multiples de δ.

Démonstration Soit u et v deux entiers relatifs. au et bv sont multiples de δ, donc $au + bv$ est multiple de δ.

Réciproquement, considérons l'ensemble A des entiers naturels non nuls qui peuvent s'écrire sous la forme $au + bv$ ($u \in \mathbb{Z}$ et $v \in \mathbb{Z}$). Si a n'est pas nul, on a : $|a| = |a|\times1 + b\times0$; 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 : $p = au' + bv'$.
Divisons a par p, on obtient : $a = pq + r$ avec $0 \leqslant r < p$. Donc : $r = a - pq = a(1 - u'q) + b(v'q)$ et $r \notin$ A ; on en déduit que : $r = 0$. Donc p divise a. De même p divise b ; donc p divise δ. Or, p est un naturel multiple de δ ; donc

:

$\delta = p = au' + bv'$.

Tout multiple de δ est de la forme : $k\delta$ ($k \in \mathbb{Z}$) ; c'est-à-dire de la forme : $a\underbrace{u'k}_{u} + b\underbrace{v'k}_{v}$ (avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$). □

Exemple On a : PGCD (300 ; 375) = 75 et 225 est multiple de 75 ;
donc il existe deux entiers relatifs u et v tels que : $225 = 300u + 375v$.
En effet : $225 = 300 \times (-3) + 375 \times 3$ ou $225 = 4\,125 - 3\,900 = 300 \times (-13) + 375 \times (11)$.

Remarque En termes ensemblistes, le théorème I.4.5 peut s'écrire : $\delta\mathbb{Z} = \{au + bv \mid u \in \mathbb{Z} \text{ et } v \in \mathbb{Z}\}$.

Exercice I.4.5. ***Soit n un entier relatif et δ le PGCD de $2n+3$ et $3n+2$. Démontrer que : $\delta = 1$ ou $\delta = 5$.***

Solution *δ divise $2n+3$ et $3n+2$, donc δ divise $3(2n+3) - 2(3n+2)$, c'est-à-dire 5. On en déduit que δ vaut 1 ou 5.* □

La démonstration du corollaire suivant est incluse dans la démonstration du théorème I.4.5.

COROLLAIRE I.4.6

Soit a et b deux entiers relatifs non tous nuls et δ leur PGCD.
Il existe deux entiers u et v tels que : $\delta = au + bv$.

Exercice I.4.6. ***L'équation : $21x - 63y = 36$; a-t-elle des solutions dans $\mathbb{Z}^2$***

Solution *21 et 63 sont deux multiples de 7. Pour tous entiers x et y le premier membre de l'équation est multiple de 7 alors que 36 n'est pas multiple de 7, l'équation n'a donc pas de solutions dans $\mathbb{Z}^2$.* □

Exercice I.4.7. ***1. Déterminer une solution, dans $\mathbb{Z}^2$, de l'équation : $7x - 24y = 1$.***
2. En déduire une solution, dans $\mathbb{Z}^2$, de l'équation : $7x - 24y = 5$.

Solution 1. *On a : $7x - 24y = 1 \iff 24y + 1 = 7x$.*
Pour trouver une solution, il suffit donc de trouver un entier y tel que $24y + 1$ soit multiple de 7. On constate que pour $y = 0$ et $y = 1$, $24y + 1$ n'est pas multiple de 7 ; en revanche pour $y = 2$ on obtient : $24y + 1 = 49 = 7 \times 7$; d'où : $7 \times 7 - 24 \times 2 = 1$.
(7 ; 2) est une solution de l'équation : $7x - 24y = 1$.

2. *En multipliant membre à membre l'égalité : $7 \times 7 - 24 \times 2 = 1$; par 5, on obtient : $7 \times 35 - 24 \times 10 = 5$.*
(35 ; 10) est une solution de l'équation : $7x - 24y = 5$;
(En utilisant la méthode précédente nous aurions trouvé une autre solution : (11 ; 3)). □

I.4.3 Déterminations du PGCD et du PPCM de deux entiers naturels

I.4.3.a Avec des nombres premiers

Soit a et b deux entiers naturels supérieurs à 1.
En mettant en commun leurs diviseurs premiers, on peut écrire :

$$a = \prod_{i=1}^{n} p_i^{\alpha_i} \qquad \text{et} \qquad b = \prod_{i=1}^{n} p_i^{\beta_i}.$$

Exemple $550 = 2 \times 5^2 \times 11$ et $405 = 3^4 \times 5$.
L'union des ensembles des diviseurs premiers de 550 et 405 est donc : {2 ; 3 ; 5 ; 11}. On a :

$$550 = 2^1 \times 3^0 \times 5^2 \times 11^1 \qquad \text{et} \qquad 405 = 2^0 \times 3^4 \times 5^1 \times 11^0$$

THÉORÈME I.4.7

Soit a et b deux entiers naturels supérieurs à 1.
En mettant en commun leurs diviseurs premiers, on peut écrire :

$$a=\prod_{i=1}^{n} p_i^{\alpha_i} \qquad \text{et} \qquad b=\prod_{i=1}^{n} p_i^{\beta_i}.$$

On a alors :

(1) $$\text{PGCD}(a,b)=\prod_{i=1}^{n} p_i^{\min\{\alpha_i,\beta_i\}} ;$$

(2) $$\text{PPCM}(a,b)=\prod_{i=1}^{n} p_i^{\max\{\alpha_i,\beta_i\}}.$$

Exemple Pour $a=550$ et $b=405$, il vient :

$$\text{PGCD}(550;405)=2^0\times 3^0\times 5^1\times 11^0=5 \qquad \text{et} \qquad \text{PGCD}(550;405)=2^1\times 3^4\times 5^2\times 11^1=44550$$

Remarque Pour tous entiers naturels α et β, on a : $\min\{\alpha,\beta\}+\max\{\alpha,\beta\}=\alpha+\beta$; on en déduit que :
$\text{PGCD}(a,b)\times\text{PPCM}(a,b)=\prod_{i=1}^{n} p_i^{\min\{\alpha_i,\beta_i\}+\max\{\alpha_i,\beta_i\}}=\prod_{i=1}^{n} p_i^{\alpha_i+\beta_i}=\prod_{i=1}^{n} p_i^{\alpha_i}\cdot\prod_{i=1}^{n} p_i^{\beta_i}=ab.$
On retrouve donc le théorème I.4.14

I.4.3.b Algorithme d'EUCLIDE

LEMME I.4.8 LEMME D'EUCLIDE

Soit a, b et q trois entiers relatifs non nuls.
On a : $\text{PGCD}(a;b)=\text{PGCD}(b;a-bq)$.

DémonstrationD'après le théorème I.2.9, on a : $\mathscr{D}(a;b)=\mathscr{D}(b;a-bq)$.
Ces deux ensembles sont égaux et bornés, ils ont donc le même plus grand élément ; d'où : $\text{PGCD}(a;b)=\text{PGCD}(b;a-bq)$.
□

Utilisons ce lemme pour déterminer le PGCD de 30621 et 92276.
Posons : $\delta=\text{PGCD}(30621;92276)$.

- Divisons 92276 par 30621 : $92276=30621\times 3+413$; donc : $\delta=\text{PGCD}(30621;413)$.
- Divisons 30621 par 413 : $30621=413\times 74+59$; donc : $\delta=\text{PGCD}(413;59)$.
- Divisons 413 par 59 : $413=59\times 7+0$; donc : $\delta=\text{PGCD}(59;0)=59$.

donc : $\delta=59$.

Dividende	92276	30621	413
Diviseur	30621	413	59
Reste	413	59	0

On peut résumer les résultats dans le tableau ci-contre. La méthode que nous avons utilisée s'appelle *algorithme d'Euclide*.

Plus généralement, on a la propriété suivante.

THÉORÈME I.4.9

Soit a et b deux entiers naturels non nuls.
Lorsque b ne divise pas a, le PGCD de a et b est le dernier reste non nul obtenu par l'algorithme d'Euclide.

Démonstration On considère la suite (r_n) telle que :
$r_0=a$ et $r_1=b$.

Si r_n n'est pas nul, alors r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n.

Si r_n est nul ; alors r_n est le dernier terme de la suite.

La suite (r_n) est une suite strictement décroissante d'entiers naturels.

Considérons l'ensemble A des nombres r_n. A est une partie non vide de $\mathbb{N}$; donc A admet un plus petit élément : r_p.

Si r_p n'était pas nul, alors r_{p+1} serait un élément de A strictement inférieur au plus petit élément de A ce qui se contredit ; donc : $r_p = 0$. On en déduit que r_{p-1} divise r_{p-2} ; donc : $\text{PGCD}\left(r_{p-2}\,;r_{p-1}\right) = r_{p-1}$.

Pour tout entier naturel k tel que : $2 \leqslant k \leqslant p-1$; on a : $\text{PGCD}\,(r_{k-2}\,;r_{k-1}) = \text{PGCD}\,(r_{k-1}\,;r_k)$.

Donc : $\text{PGCD}\,(r_0\,;r_1) = \text{PGCD}\left(r_{p-2}\,;r_{p-1}\right)$. C'est-à-dire : $\text{PGCD}\,(a\,;b) = r_{p-1}$. □

I.4.4 Nombres premiers entre eux

I.4.4.a Définition et propriétés

DÉFINITION I.4.3

Deux entiers *premiers entre eux* sont deux entiers dont le PGCD est 1.

Exemples

1. On a vu que : $\text{PGCD}\,(7\,;24) = 1$; donc 7 et 24 sont premiers entre eux.

2. 42 et 77 sont tous les deux divisibles par 7 ; donc ils ne sont pas premiers entre eux.

Remarques

1. Certains utilisent l'expression « *nombres étrangers* » pour nombres premiers entre eux.

2. Soit a et b deux entiers relatifs non tous nuls et d un diviseur commun à a et b.

On a : $a = da'$ (avec $a' \in \mathbb{Z}$) ; $b = db'$ (avec $b' \in \mathbb{Z}$) et $\text{PGCD}\,(a\,;b) = d\,\text{PGCD}\left(a'\,;b'\right)$.

d est le PGCD de a et b si et seulement si a' et b' sont premiers entre eux.

3. Dire qu'une fraction est irréductible signifie que le numérateur et le dénominateur sont premiers entre eux.

4. Les seuls diviseurs communs de deux nombres premiers entre eux sont -1 et 1.

THÉORÈME I.4.10 THÉORÈME DE BÉZOUT[1] -BACHET[2]

Soit a et b deux entiers relatifs.

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

Démonstration

Si a et b sont premiers entre eux alors leur PGCD est 1 et donc, d'après le théorème I.4.5, il existe deux entiers relatifs u et v tels que : $au + bv = 1$.

Réciproquement, soit δ le PGCD de a et b. S'il existe deux entiers relatifs u et v tels que : $au + bv = 1$, alors δ divise $au + bv$ et donc 1 ; or 1 divise δ de plus 1 et δ sont positifs, donc : $\delta = 1$; c'est-à-dire : a et b sont premiers entre eux. □

Exemples

1. On a : $632 \times 9 + 47 \times (-121) = 1$; donc : 632 et 47 sont premiers entre eux.

2. Deux entiers consécutifs n et $n+1$ sont premiers entre eux.

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

COROLLAIRE I.4.11

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

Si a est premier avec b et c, alors a est premier avec bc.

DémonstrationD'après le théorème de BÉZOUT-BACHET (I.4.10), 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 : $a(auu' + cuv' + bvu') + bc \times vv' = 1$.

Donc, d'après le théorème de BÉZOUT-BACHET, a est premier avec bc. □

Exercice I.4.8. ***Soit n un entier relatif, démontrer que $7n+18$ et $10n^2+51n+65$ sont premiers entre eux (on pourra factoriser $10n^2+51n+65$).***

Solution *En factorisant, on obtient :* $10n^2+51n+65=(5n+13)(2n+5)$.
On a : $2(7n+18)-7(2n+5)=1$ *et* $-5(7n+18)+7(5n+13)=1$ *; donc, d'après le théorème de* BÉZOUT, $7n+18$ *est premier avec* $2n+5$ *et* $5n+13$ *; par conséquent* $7n+18$ *est premier ave leur produit c'est-à-dire* $10n^2+51n+65$. □

Exercice I.4.9. ***a est un entier premier avec 3 et 7, l'équation : $ax-21y=5$; a-t-elle au moins une solution ?***

Solution *a est premier avec* 3 *et avec* 7, *donc a et* 21 *sont premiers entre eux, d'où :* $\text{PGCD}(a,21)=1$. *Lorsque* (x,y) *décrit* $\mathbb{Z}^2$, $ax-21y$ *décrit l'ensemble des multiples de* $\text{PGCD}(a,21)$, *c'est-à-dire* $\mathbb{Z}$, *donc l'équation a au moins une solution.* □

THÉORÈME I.4.12 **THÉORÈME DE GAUSS**[3]

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 : $a(uc+kv)=c$. Par conséquent a divise c. □

Exercice I.4.10. ***Résoudre dans $\mathbb{Z}^2$ l'équation :***

$$\mathbf{7x-3y=0} \tag{I.3}$$

Solution *Soit* (x,y) *une solution de* (I.3). *On a :* $7x=3y$.
7 *divise* $3y$ *et est premier avec* 3, *donc, d'après le théorème de* GAUSS, y *est multiple de* 7.
Il existe donc un entier relatif k tel que : $y=7k$. *On en déduit que :* $x=3k$.

Réciproquement, pour tout entier relatif k, on a : $7(3k)-3(7k)=0$ *; donc le couple* $(3k;7k)$ *est solution de* (I.3).

L'ensemble des solutions est donc : $\{(3k;7k)\,|\,k\in\mathbb{Z}\}$. □

COROLLAIRE I.4.13

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

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

(2) Si a et b sont premiers entre eux, alors : $\text{PPCM}(a;b)=|ab|$.

Démonstration

(1) Il existe un entier relatif a' tel que : $c=aa'$. b divise aa' et est premier avec a ; donc, d'après le théorème de GAUSS, il existe un entier relatif b' tel que : $a'=bb'$.
On en déduit que : $c=abb'$; donc ab divise c.

(2) a et b divisent $\text{PPCM}(a;b)$ et a et b sont premiers entre eux, donc ab divise $\text{PPCM}(a;b)$.
ab est multiple de a et de b, donc ab est multiple de $\text{PPCM}(a;b)$. On en déduit que : $\text{PPCM}(a;b)=|ab|$. □

Exercice I.4.11. ***Soit n un entier relatif, démontrer que n^3-n est multiple de 6.***

Solution *On a :* $n^3-n=n(n^2-1)=(n-1)\times n\times(n+1)$ *; n^3-n est donc le produit de trois entiers consécutifs, l'un d'entre eux est multiple de* 3, *donc n^3-n est multiple de* 3.

$n\times(n+1)$ *est le produit de deux entiers consécutifs, l'un deux est multiple de* 2, *donc n^3-n est multiple de* 2.

n^3-n *est multiple de* 2 *et de* 3, *de plus* 2 *et* 3 *sont premiers entre eux donc n^3-n est multiple de* 6. □

Exercice I.4.12. ***Soit n un entier naturel non nul, déterminer le PPCM de n et $n+1$.***

Solution *n et $n+1$ sont deux entiers consécutif donc , d'après le théorème de* BÉZOUT, *ils sont premiers entre eux et donc :* $\text{PPCM}(n;n+1)=n(n+1)$. □

I.4.4.b Relation entre le PGCD et le PPCM de deux entiers naturels

THÉORÈME I.4.14

Soit a et b deux entiers naturels non nuls, δ leur PGCD et μ leur PPCM.
On a : $\delta\mu = ab$.

Démonstration Les entiers naturels a' et b' tels que : $a = \delta a'$ et $b = \delta b'$ sont premiers entre eux.
Donc : $\text{PPCM}(a;b) = \delta\,\text{PPCM}(a';b') = \delta a'b'$. On en déduit, en multipliant membre à membre par δ, que : $\delta\mu = ab$. □

Exercice I.4.13. ***Déterminer le PPCM de 30 621 et 92 276.***

Solution *On a vu que :* $\text{PGCD}(30\,621;92\,276) = 59$ *;*
donc : $\text{PPCM}(30\,621;92\,276) = \dfrac{30\,621 \times 92\,276}{59} = 47\,891\,244$. □

I.4.5 Équations diophantiennes

L'objectif de cette partie est de montrer comment résoudre des équations diophantiennes de degré 1 à deux inconnues ; c'est-à-dire les équations du type :

$$ax + by = c$$

où les inconnues sont les entiers x et y et où a, b, c sont des paramètres entiers. Par exemple, résoudre dans $\mathbb{Z}^2$ l'équation : $2x + 3y = 7$.

Nous allons d'abord étudier des exemples simples, nous constaterons alors que résoudre une telle équation il faut souvent trouver une solution puis on déduit les autres solutions de cette solution particulière. Nous verrons donc comment déterminer une solution particulière dans le cas où les coefficients sont compliqués.

I.4.5.a Exemples de résolutions

Exercice I.4.14. ***Résoudre dans $\mathbb{Z}^2$ l'équation : $25x + 15y = 7$.***

Solution *Pour tous entiers x et y, $25x+15y$ est multiple de 5 (car 25 et 15 sont multiples de 5) alors que 7 ne l'est pas, donc l'équation n'a pas de solution.* □

Exercice I.4.15. ***Résoudre dans $\mathbb{Z}^2$ l'équation :***

$$\mathbf{25x + 15y = 35.} \tag{I.4}$$

Solution *On a :* (I.4) $\iff$ $5x + 3y = 7$.
On a : $5 \times 2 + 3 \times (-1) = 10 - 3 = 7$ *; donc* $(2;-1)$ *est une solution particulière de* (I.4).
d'où : (I.4) $\iff$ $5x + 3y = 5 \times 2 + 3 \times (-1)$
$\iff$ $3(y+1) = -5(x-2)$.
Raisonnons maintenant par conditions nécessaires. Soit $(x;y)$ une solution.
3 divise $-5(x-2)$ et est premier avec -5 donc, d'après le théorème de GAUSS, *3 divise $x-2$.*
Soit k le quotient, on a donc : $x-2 = 3k$ et $x = 3k+2$.
En substituant $x-2$ par $3k$ dans le dernier membre de la dernière équivalence, il vient : $3(y+1) = -5 \times 3k$ *; d'où :* $y = -5k-1$.
On en déduit que toutes les solutions de (I.4) *sont de la forme :* $(3k+2;-5k-1)$ *(avec $k \in \mathbb{Z}$).*

Réciproquement, les couples de cette forme sont-ils tous solutions de (I.4) *?*
Soit $k \in \mathbb{Z}$*, considérons le couple* $(3k+2;-5k-1)$.
On a : $5(3k+2)+3(-5k-1)=15k+10-15k-3=7$ *; donc :*

$$\boxed{S=\{(3k+2;-5k-1)\,|\,k\in\mathbb{Z}\}}.$$

□

I.4.5.b Détermination d'une solution particulière

Exercice I.4.16. ***On se propose de déterminer une solution particulière de l'équation :*** $567x+2\,854y=5$.

1. Démontrer, en utilisant l'algorithme d'Euclide, que 567 ***et*** 2 854 ***sont premiers entre eux.***

2. Utiliser les calculs effectués à la question précédente pour déterminer deux entiers relatifs u ***et*** v ***tels que :*** $567u+2\,854v=1$.

3. Déterminer deux réels u' ***et*** v' ***tels que :*** $567u'+2\,854v'=5$.

Solution 1. *On a :* $2\,854=5\times567+19$ *; donc :* $\text{PGCD}(2\,854;567)=\text{PGCD}(567;19)$.
On a : $567=29\times19+16$ *; donc :* $\text{PGCD}(567;19)=\text{PGCD}(19;16)$.
On a : $19=16+3$ *; donc :* $\text{PGCD}(19;16)=\text{PGCD}(16;3)$.
On a : $16=5\times3+1$ *; donc :* $\text{PGCD}(16;3)=\text{PGCD}(3;1)=1$.
Les nombres 567 *et* 2 854 *sont donc premiers entre eux.*

2. *Utilisons les divisions euclidiennes précédentes, de la dernière à la première.*
On a :
$$\begin{aligned}1&=16-5\times3\\&=16-5(19-16)\\&=-5\times19+6\times16\\&=-5\times19+6(567-29\times19)\\&=6\times567-179\times29\\&=6\times567-179(2\,854-5\times567)\\&=901\times567-179\times2\,854\end{aligned}$$
On peut donc prendre : $u=901$ *et* $v=-179$.

3. *En multipliant membre à membre le dernière égalité par 5, nous obtenons :*

$$4\,505\times567-895\times2\,854=5.$$

On peut donc prendre : $u'=4\,505$ *et* $v'=-895$. □

I.4.6 Exercices

I.4.a. Déterminer le PPCM des entiers relatifs a et b dans chacun des cas suivants.
$a=60$ et $b=15$; $a=35$ et $b=91$;
$a=-5$ et $b=13$; $a=512$ et $b=896$.

I.4.b. Déterminer le PGCD des entiers relatifs a et b dans chacun des cas suivants.
$a=17$ et $b=17$; $a=-13$ et $b=39$;
$a=99$ et $b=56$; $a=729$ et $b=405$.

I.4.c. À l'aide de l'algorithme d'EUCLIDE, déterminer le PGCD de 676 et 2 002.

I.4.d. À l'aide du théorème de BÉZOUT, démontrer que pour tout entier relatif n, $2n+5$ et $5n+13$ sont premiers entre eux.

I.4.e. À l'aide du lemme d'EUCLIDE, démontrer que pour tout entier relatif n, $2n+5$ et $5n+13$ sont premiers entre eux.

I.4.f. Soit a et b deux entiers tous non nuls et n un entier tel que : $n\geqslant2$.
1. Démontrer que si a^n et b^n sont premiers entre

eux, alors a et b sont premiers entre eux.

2. Démontrer que : $\text{PGCD}\left(a^n, b^n\right) = \text{PGCD}^n(a,b)$.

I.4.g. Résoudre dans $\mathbb{Z}^2$ l'équation : $7x-3y=4$

I.4.h. Résoudre dans $\mathbb{Z}^2$ l'équation : $256x - 121y = 3$

I.5 Congruence modulo n

I.5.1 Définition et propriétés immédiates

DÉFINITION I.5.1

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 : $a \equiv b \ (n)$; $a \equiv b$ (modulo n) ; $a \equiv b \,(\text{mod}\, n)$ ou parfois $a \equiv b \ [n]$.

Exemples

1. $56 \equiv 6 \,(\text{mod}\, 10)$; car : $56-6=50=5\times 10$.
2. $77 \equiv 0 \,(\text{mod}\, 7)$; car : $77-0=77=11\times 7$.
3. $-5 \equiv 3 \,(\text{mod}\, 8)$; car : $-5-3=-8=-1\times 8$.

Remarques

1. a est multiple de n si et seulement si : $a \equiv 0 \,(\text{mod}\, n)$.
2. $a \equiv b \ (n)$ signifie $a-b \in n\mathbb{Z}$
3. Si r désigne le reste de la division euclidienne de a par n, alors : $a \equiv r \,(\text{mod}\, n)$.

Les propriétés suivantes sont des conséquences immédiates de la définition.

THÉORÈME I.5.1

Soit n un entier naturel non nul et a, b, c trois entiers relatifs.

(1)	$a \equiv a \,(\text{mod}\, n)$	La congruence modulo n est réflexive.
(2)	$a \equiv b \,(\text{mod}\, n) \iff b \equiv a \,(\text{mod}\, n)$	La congruence modulo n est symétrique.
(3)	$\begin{cases} a \equiv b \,(\text{mod}\, n) \\ b \equiv c \,(\text{mod}\, n) \end{cases} \implies a \equiv c \,(\text{mod}\, n)$	La congruence modulo n est transitive.

On dit que la congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Remarque On a déjà rencontré des relations d'équivalences, par exemple : dans l'ensemble des droites du plan la relation « est parallèle à ».

I.5.1.a Autres propriétés

THÉORÈME I.5.2

Soit n un entier naturel non nul.
Deux entiers sont congrus modulo n si et seulement si ils ont le même reste lorsqu'on les divise par n.

Démonstration soit a et a' deux entiers relatifs et r, r' les restes respectifs des divisions euclidiennes de a et a' par n.
Démontrons que si : $r=r'$; alors : $a \equiv a' \,(\text{mod}\, n)$. Supposons que : $r=r'$; alors : $r \equiv r' \,(\text{mod}\, n)$.
Or on sait que : $a \equiv r \,(\text{mod}\, n)$ et $r' \equiv a' \,(\text{mod}\, n)$; donc par transitivité : $a \equiv a' \,(\text{mod}\, n)$.

Réciproquement, démontrons que si : $a \equiv a' \pmod{n}$; alors : $r = r'$.

Supposons que : $a \equiv a' \pmod{n}$. On sait que : $r \equiv a \pmod{n}$ et $a' \equiv r' \pmod{n}$;

donc par transitivité : $r \equiv r' \pmod{n}$; ce qui signifie qu'il existe un entier k tel que : $r - r' = kn$.

Or : $0 \leqslant r < n$ et $-n < -r' \leqslant 0$; donc par somme : $-n < r - r' < n$; d'où, en divisant par n $(n > 0)$: $-1 < k < 1$.

Par conséquent $k = 0$ et donc : $r = r'$. □

THÉORÈME I.5.3

Soit n un entier naturel non nul et a, a', b, b' quatre entiers relatifs.

(1) Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors $a + b \equiv a' + b' \pmod{n}$.

(2) Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors $ab \equiv a'b' \pmod{n}$.

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

Démonstration

$$\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases} \Longrightarrow \begin{cases} a - a' \in n\mathbb{Z} \\ b - b' \in n\mathbb{Z} \end{cases} \Longrightarrow (a - a') + (b - b') \in n\mathbb{Z} \Longrightarrow (a + b) - (a + b') \in n\mathbb{Z} \Longrightarrow a + b \equiv a' + b' \pmod{n}$$

$$\begin{cases} a \equiv a' \pmod{n} \\ b \equiv b' \pmod{n} \end{cases} \Longrightarrow \begin{cases} a - a' \in n\mathbb{Z} \\ b - b' \in n\mathbb{Z} \end{cases} \Longrightarrow b(a - a') - a'(b - b') \in n\mathbb{Z} \Longrightarrow ab - a'b' \in n\mathbb{Z} \Longrightarrow ab \equiv a'b' \pmod{n}$$

□

Remarques

1. Pour $b = b'$, on obtient :

$a \equiv a' \pmod{n} \Longrightarrow a + b \equiv a' + b \pmod{n}$ et $a \equiv a' \pmod{n} \Longrightarrow ab \equiv a'b \pmod{n}$.

2. En ce qui concerne le produit, la réciproque de l'implication est fausse ; en effet :

$4 \times 2 \equiv 7 \times 2 \pmod{6}$; et pourtant : $4 \not\equiv 7 \pmod{6}$.

Exercice I.5.1. ***On considère les nombres a et b tels que : a = 135 et b = 93.***

Déterminer le reste de la division euclidienne de a + b, ab et 2a − 3b par 23.

Solution *On a : $a \equiv 20 \pmod{23}$ et $b \equiv 1 \pmod{23}$.*

Donc : $a + b \equiv 21 \pmod{23}$.

Or : $0 \leqslant 21 < 23$; donc 21 est le reste de la division euclidienne de $a + b$ par 23.

De même : $ab \equiv 20 \pmod{23}$.

Or : $0 \leqslant 20 < 23$; donc 20 est le reste de la division euclidienne de ab par 23.

De même : $2a - 3b \equiv 39 \pmod{23}$; donc : $2a - 3b \equiv 16 \pmod{23}$.

Or : $0 \leqslant 16 < 23$; donc 16 est le reste de la division euclidienne de $2a - 3b$ par 23. □

COROLLAIRE I.5.4

Soit a et b deux entiers relatifs et k, n deux entiers naturels non nuls.

(1) Si : $a \equiv b \pmod{n}$; alors : $a^k \equiv b^k \pmod{n}$.

(2) $b^k - a^k$ est multiple de $b - a$.

Démonstration(1) Pour $k = 1$, la propriété est immédiate.

Supposons la vraie pour un certain k, on a alors : $a \equiv b \pmod{n}$ et $a^k \equiv b^k \pmod{n}$; donc par produit : $a^{k+1} \equiv b^{k+1} \pmod{n}$.

Par récurrence, on en déduit la propriété pour tout entier naturel non nul k.

(2) La propriété est immédiate lorsque $a = b$, on suppose donc désormais que : $a \neq b$.

$b - a$ est multiple de $|b - a|$ et $|b - a| \neq 0$, donc : $b \equiv a \pmod{|b - a|}$; d'où : $b^k \equiv a^k \pmod{|b - a|}$; de qui signifie que $b^k - a^k$ est multiple de $|b - a|$ et donc de $b - a$. □

Remarques

1. On pouvait également voir la propriété (2) du corollaire ci-dessus comme une conséquence immédiate de l'identité remarquable établie au corollaire **??** page **??**.

2. Lorsque les nombres a et b sont tous non nuls, le corollaire I.5.4 est vrai pour k =0.

Exercice I.5.2. ***Démontrer que pour tout enter naturel n, $5^{3n}-2^{2n}$ est multiple de 121.***

Solution *Soit n un enter naturel. On a :* $5^{3n}-2^{2n}=\left(5^3\right)^n-\left(2^2\right)^n=125^n-4^n$.
On sait que 125^n-4^n *est multiple de* $125-4$, *donc* $5^{3n}-2^{2n}$ *est multiple de* 121. □

THÉORÈME I.5.5

Soit n un entier naturel non nul et a, b et c trois entiers relatifs.
Si a est premier avec n alors :

$$ab\equiv ac\,(\mathrm{mod}\,n)\qquad\Longleftrightarrow\qquad b\equiv c\,(\mathrm{mod}\,n)\,.$$

Démonstration Si : $ab\equiv ac\,(\mathrm{mod}\,n)$; alors n divise $ab-ac$.
n divise $a(b-c)$ et est premier avec a d0onc, d'après le théorème de GAUSS, n divise $b-c$; ce qui signifie que : $b\equiv c\,(\mathrm{mod}\,n)$.
L'implication réciproque est un corollaire du théorème I.5.3. □

I.5.2 Petit théorème de FERMAT

THÉORÈME I.5.6 **PETIT THÉORÈME DE FERMAT**

Soit p un nombre premier et a un entier relatif.
(1) $$a^p\equiv a\left(\mathrm{mod}\,p\right);$$
(2) si de plus a et p sont premiers entre eux alors :
$$a^{p-1}\equiv 1\left(\mathrm{mod}\,p\right).$$

Démonstration
(1) Si a est premier avec p, la propriété se déduit de **(2)** en multipliant membre à membre par a ; sinon a n'est premier avec p alors a et a^p sont multiples de p et la propriété est également vérifiée. Il suffit donc de démontrer la propriété **(2)**.
(2) L'ensemble des restes non nuls modulo p est : $[\![1,p-1]\!]$.
Soit f l'application de $[\![1,p-1]\!]$ dans lui-même qui à tout $r\in[\![1,p-1]\!]$ associe le reste modulo p de ar.
On se propose de démontrer que f est une bijection.
Soit r et r' deux élément distincts de $[\![1,p-1]\!]$, $(r'-r)$ n'est pas multiple de p, il est donc premier avec p, de plus a est premier avec p donc $ar-ar'$ n'est pas multiple de p, on en déduit que : $f(r)\neq f(r')$.

$$r\neq r'\qquad\Longrightarrow\qquad f(r)\neq f(r')\tag{I.5}$$

Soit $\rho\in[\![1,p-1]\!]$. Supposons que ρ n'est pas d'antécédent par f ; l'image de $[\![1,p-1]\!]$ par f serait incluse dans $[\![1,p-1]\!]\setminus\{\rho\}$ et donc deux éléments (au moins) de $[\![1,p-1]\!]$ auraient la même image ce qui est en contradiction avec I.5. On en déduit que ρ a un antécédent par f et d'après I.5 cet antécédent est unique.
Donc f est une bijection.
Par commutativité de la multiplication, il vient :

$$\prod_{r\in[\![1,p-1]\!]}f(r)=\prod_{r\in[\![1,p-1]\!]}r=(p-1)!$$

Pour tout $r\in[\![1,p-1]\!]$ on a : $ar\equiv f(r)\left(\mathrm{mod}\,p\right)$; donc par produit :

$$a^{p-1}(p-1)!\equiv\prod_{r\in[\![1,p-1]\!]}f(r)\left(\mathrm{mod}\,p\right)$$

c'est-à-dire

$$a^{p-1}(p-1)!\equiv(p-1)!\left(\mathrm{mod}\,p\right)$$

p est est premier avec tous les élément de $[\![1,p-1]\!]$, il donc premier avec leur produit, $(p-1)!$, on en déduit par quotient que :

$$a^{p-1}\equiv 1\left(\mathrm{mod}\,p\right).$$

□

Remarque Ce théorème peut s'énoncer en disant que $a^p - a$ est multiple de p et que si a est n'est pas multiple de p alors $a^{p-1} - 1$ est multiple de p.

Exercice I.5.3. ***Démontrer que pour tout entier relatif n, $n^7 - n$ est multiple de 42.***

Solution *Soit n un entier relatif.*
7 est un nombre premier donc, d'après le petit théorème de FERMAT, *$n^7 - n$ est multiple de 7.*
On a : $n^7 - n = n\left(\left(n^2\right)^3 - 1\right) = \left(n^3 - n\right)\left(n^4 + n^2 + 1\right)$;
3 est premier, donc $n^3 - n$ est multiple de 3 or $n^7 - n$ est multiple de $n^3 - n$, donc $n^7 - n$ est multiple de 3. $n^7 - n$ est multiple de 3 et de 7, qui sont premiers entre eux, donc $n^7 - n$ est multiple de 21.
On a : $n^7 - n = n(n-1)\left(n^6 + n^5 + n^4 + n^3 + n^2 + n + 1\right) = \left(n^2 - n\right)\left(n^6 + n^5 + n^4 + n^3 + n^2 + n + 1\right)$;
2 est premier, donc $n^2 - n$ est multiple de 2 or $n^7 - n$ est multiple de $n^2 - n$, donc $n^7 - n$ est multiple de 2. $n^7 - n$ est multiple de 2 et de 21, qui sont premiers entre eux, donc $n^7 - n$ est multiple de 42.
□

I.5.3 Résolution d'équations avec congruences

Dans toute cette partie n désigne un entier naturel non nul.

I.5.3.a Équations du type : $ax \equiv 1 \pmod{n}$

Dans $\mathbb{R}$ deux nombres inverses l'un de l'autre sont deux nombres dont le produit est 1.
Lorsque deux entiers a et u vérifient : $au \equiv 1 \pmod{n}$; on dira que a et u sont « inverses » modulo n.

Exemples

1. On a : $3 \times 4 \equiv 1 \pmod{11}$; donc 3 et 4 sont « inverses » modulo 11.
2. On a : $3 \times 15 = 45 = 1 + 4 \times 11$; d'où : $3 \times 15 \equiv 1 \pmod{11}$; donc 3 et 15 sont « inverses » modulo 11.
3. On a : $3 \times (-7) = -21 = 1 - 2 \times 11$; d'où : $3 \times -7 \equiv 1 \pmod{11}$; donc 3 et -7 sont « inverses » modulo 11.

Dans $\mathbb{R}$, pour résoudre l'équation $3x = 1$ on multiplie membre à membre par l'inverse de 3.

Exercice I.5.4. ***Résoudre dans $\mathbb{Z}$:***

$$\mathbf{3x \equiv 1 \pmod{11}} \tag{I.6}$$

Solution *4 est premier avec 11, donc (d'après I.5.5) :*

$$\text{(I.6)} \iff 4 \times 3x \equiv 4 \times 1 \pmod{11} \iff 12x \equiv 4 \pmod{11}.$$

On a : $12 \equiv 1 \pmod{11}$; donc pour tout entier x : $12x \equiv x \pmod{11}$;
on en déduit que : $\text{(I.6)} \iff x \equiv 4 \pmod{11}$.

$$S = \left\{11k + 4 \,\middle|\, k \in \mathbb{Z}\right\}$$

□

Remarque Un entier a a des « inverses », u, modulo n si et seulement si il est premier avec n. En effet : $au \equiv 1 \pmod{n}$; signifie qu'il existe un entier v tel que : $au + nv = 1$; on reconnaît l'identité de BÉZOUT et on en déduit le résultat.

Exercice I.5.5. ***Résoudre dans $\mathbb{Z}$: $15x \equiv 1 \pmod 9$***

Solution *Un entier x est solution de l'équation si et seulement si il existe un entier k tel que :* $15x - 9k = 1$.
Le premier membre de l'égalité est multiple de 3 *et le second ne l'est pas donc :*

$$S = \varnothing$$

□

I.5.3.b Équations du type : $ax \equiv b \pmod n$

THÉORÈME I.5.7

Soit a et b deux entiers relatifs et n un entier naturel non nul.
l'équation : $ax \equiv b \pmod n$; a au moins une solution si et seulement si b est multiple du PGCD de a et n.

Démonstration Un entier x est solution de l'équation si et seulement si il existe un entier k tel que : $ax - nk = b$.
D'après le théorème I.4.5 les nombres de la forme $ax - nk$ sont les multiples du PGCD de a et n. □

Remarques

1. En pratique dès que l'équation a une solution, elle en a une infinité.
2. Dès que a et n sont premiers entre eux, elle en a donc une infinité.

Dans le cas où a et n sont premiers entre eux, pour résoudre une telle équation, il suffit de connaître une solution particulière.

Exercice I.5.6. ***Résoudre dans $\mathbb{Z}$: $5x \equiv 7 \pmod{11}$.***

Solution *On a :* $5 \times 8 = 40 = 7 + 11 \times 3$ *; donc :* $5 \times 8 \equiv 7 \pmod{11}$.
8 *est donc une solution particulière de l'équation, on en déduit que :*

$$\begin{aligned} 5x \equiv 7 \pmod{11} &\iff 5x \equiv 5 \times 8 \pmod{11} \\ &\iff 5(x-8) \equiv 0 \pmod{11} \\ &\iff x - 8 \equiv 0 \pmod{11} \qquad \text{car } 5 \text{ et } 11 \text{ sont premiers entre eux} \\ &\iff x \equiv 8 \pmod{11}. \end{aligned}$$

$$S = \{11k + 8 \,|\, k \in \mathbb{Z}\}$$

□

On peut également utiliser un « inverse » de a modulo n.

Exercice I.5.7. ***Résoudre dans $\mathbb{Z}$: $5x \equiv 7 \pmod{11}$.***

Solution

$$\begin{aligned} 5x \equiv 7 \pmod{11} &\iff 9 \times 5x \equiv 9 \times 7 \pmod{11} \qquad \text{car } 9 \text{ et } 11 \text{ sont premiers entre eux} \\ &\iff 45x \equiv 63 \pmod{11} \\ &\iff x \equiv -3 \pmod{11}. \qquad \text{car } 45 \equiv 1 \pmod{11} \text{ et } 63 \equiv -3 \pmod{11} \end{aligned}$$

$$S = \{11k + 8 \,|\, k \in \mathbb{Z}\}$$

□

Dans le cas où a et n ne sont pas premiers entre eux, pour résoudre une telle équation, on se ramène au où ils sont premiers entre eux.

Exercice I.5.8. ***Résoudre dans $\mathbb{Z}$: $15x \equiv 25 \pmod{10}$.***

Solution

$$\begin{aligned}
15x \equiv 25 \pmod{10} &\iff 15x = 25 + 35k \quad (k \in \mathbb{Z}) \\
&\iff 3x = 5 + 7k \quad (k \in \mathbb{Z}) \\
&\iff 3x \equiv 5 \pmod{7} \\
&\iff 3x \equiv 3 \times 4 \pmod{7} && \text{car } 5 \equiv 3 \times 4 \pmod{7} \\
&\iff 3(x-4) \equiv 0 \pmod{7} \\
&\iff x - 4 \equiv 0 \pmod{7} && \text{car } 3 \text{ et } 7 \text{ sont premiers entre eux} \\
&\iff x \equiv 4 \pmod{7}.
\end{aligned}$$

$$S = \{7k + 4 \,|\, k \in \mathbb{Z}\}$$

□

I.5.3.c Système d'équations

L'objectif de cette partie est de montrer, à travers des exemples, comment résoudre un système du type :

$$\begin{cases} ax \equiv b \pmod{m} \\ cx \equiv d \pmod{n} \end{cases}.$$

Lorsque $a = c = 1$ il suffit de remarquer une solution particulière.

Exercice I.5.9. ***Résoudre dans $\mathbb{Z}$ le système :*** $\begin{cases} \boldsymbol{x \equiv 7 \pmod{8}} \\ \boldsymbol{x \equiv 11 \pmod{12}} \end{cases}$.

Solution *On remarque que -1 est une solution du système.*

$$\begin{cases} x \equiv 7 \pmod{8} \\ x \equiv 11 \pmod{12} \end{cases} \iff \begin{cases} x \equiv -1 \pmod{8} \\ x \equiv -1 \pmod{12} \end{cases} \iff \begin{cases} x + 1 \equiv 0 \pmod{8} \\ x + 1 \equiv 0 \pmod{12} \end{cases}.$$

Les solutions du système sont les entiers x tels que $x+1$ est à la fois multiple de 8 et 12, c'est-à-dire de leur PPCM : 24. D'où :

$$\boxed{S = \{\boldsymbol{24k - 1} \,|\, \boldsymbol{k} \in \mathbb{Z}\}}.$$

□

Il se peut toutefois qu'on ne remarque pas de solution particulière. On peut alors en trouver une en déterminant une solution particulière d'une équation diophantienne associée au système.

Exercice I.5.10. ***Résoudre dans $\mathbb{Z}$ le système :*** $\begin{cases} \boldsymbol{x \equiv 7 \pmod{129}} \\ \boldsymbol{x \equiv 11 \pmod{1223}} \end{cases}$.

Solution *Soit x une solution (s'il en existe). Il existe alors deux entiers a et b tels que : $x = 129a + 7$ et $x = 1223b + 11$; le couple vérifie donc :*

$$129a - 1223b = 4.$$

*On appliquant l'algorithme d'*EUCLIDE *et en remontant de proche en proche (voir exercice I.4.16.), il vient : $493 \times 129 - 52 \times 1223 = 1$; d'où, par produit par 4 : $1972 \times 129 - 208 \times 1223 = 4$.*
$(a;b) = (1972;208)$ est une solution particulière de l'équation.
On a : $1972 \times 129 + 7 = 208 \times 1223 + 11$; donc : $129a + 7 = 1972 \times 129 + 7 = 254395$; est une solution du système.
On a donc :

$$\begin{cases} x \equiv 7 \pmod{129} \\ x \equiv 11 \pmod{1223} \end{cases} \iff \begin{cases} x \equiv 254395 \pmod{129} \\ x \equiv 254395 \pmod{1223} \end{cases}$$

$$\iff \begin{cases} x - 254395 \equiv 0 \pmod{129} \\ x - 254395 \equiv 0 \pmod{1223} \end{cases}.$$

Les solutions du système sont les entiers x tels que $x-254395$ est à la fois multiple de 129 et 1223, c'est-à-dire de leur PPCM : 157767 *(qu'il aurait fallu calculer)). D'où :*

$$\boxed{S=\{\mathbf{157767}k+\mathbf{254395}\,|\,k\in\mathbb{Z}\}}.$$

□

Si on est pas dans le cas $a=c=1$, alors on peut s'y ramener.

Exercice I.5.11. ***Résoudre dans $\mathbb{Z}$ le système :*** $\begin{cases}15x\equiv 9\,(\text{mod}\,12)\\4x\equiv 5\,(\text{mod}\,7)\end{cases}$.

Solution $15x\equiv 9\,(\text{mod}\,12) \iff 15x=9+12k\ (k\in\mathbb{Z})$
$\iff 5x=3+4k\ (k\in\mathbb{Z})$
$\iff 5x\equiv 3\,(\text{mod}\,4)$
$\iff x\equiv 3\,(\text{mod}\,4)$

$4x\equiv 5\,(\text{mod}\,7) \iff 8x\equiv 10\,(\text{mod}\,7)$
$\iff x\equiv 3\,(\text{mod}\,7)$

Donc : $\begin{cases}15x\equiv 9\,(\text{mod}\,12)\\4x\equiv 5\,(\text{mod}\,7)\end{cases} \iff \begin{cases}x-3\equiv 0\,(\text{mod}\,4)\\x-3\equiv 0\,(\text{mod}\,7)\end{cases}$.

Les soltutions du système sont les entiers x tels que $x-3$ est à la fois multiple de 4 et de 7 donc de leur PPCM : 28.

$$\boxed{S=\{\mathbf{28}k+\mathbf{3}\,|\,k\in\mathbb{Z}\}}.$$

□

I.5.3.d Équations polynomiales

Pour résoudre une équation du type : $p(x)\equiv 0\,(\text{mod}\,n)$; on peut chercher un polynôme congru à p dont les racines sont entières.

Exercice I.5.12. ***Résoudre dans $\mathbb{Z}$ l'équation : $x^2\equiv 7\,(\text{mod}\,9)$.***

Solution *On a :* $7\equiv 16\,(\text{mod}\,9)$ *; donc :*

$$x^2\equiv 7\,(\text{mod}\,9) \iff x^2-16\equiv 0\,(\text{mod}\,9) \iff (x-4)(x+4)\equiv 0\,(\text{mod}\,9).$$

Un entier x est solution de l'équation si et seulement si $(x-4)(x+4)$ est multiple de 9, mais $9=3^2$; on a donc trois possibilités. Soit $x-4$ est multiple de 9, soit $(x+4)$ est multiple de 9, soit $(x-4)$ et $(x+4)$ sont multiples de 3. La dernière possibilité n'est pas envisageable car on en déduirait que $(x+4)-(x-4)$, c'est-à-dire 8, est multiple de 3 ; donc :

$$\boxed{S=\{\mathbf{9}k+\mathbf{4}\,|\,k\in\mathbb{Z}\}\cup\{\mathbf{9}k+\mathbf{4}\,|\,k\in\mathbb{Z}\}}.$$

□

On peut aussi envisager tous les cas possibles.

Exercice I.5.13. ***Résoudre dans $\mathbb{Z}$ l'équation : $x^3-13x^2-5x+7\equiv 0\,(\text{mod}\,3)$.***

Solution

1$^{\text{er}}$ cas : $x\equiv 0\,(\text{mod}\,3)$

x^3-13x^2-5x est multiple de x qui lui-même est multiple de 3, donc : $x^3-13x^2-5x+7\equiv 7\,(\text{mod}\,3)$; c'est-à-dire : $x^3-13x^2-5x+7\equiv 1\,(\text{mod}\,3)$. x n'est donc pas solution.

2$^{\text{e}}$ cas : $x\equiv 1\,(\text{mod}\,3)$

x, x^2, x^3 et x^4 sont congrus à 1 modulo 3 donc par combinaisons : $x^3-13x^2-5x+7\equiv 1-13-5-7\,(\text{mod}\,3)$; c'est-à-dire : $x^4-13x^3-7x^2-2x\equiv 0\,(\text{mod}\,3)$. x est solution.

3^e cas : $x \equiv 2 \pmod 3$

x^2 est congru à 1 modulo 3 alors x et x^3 sont congrus à -1 modulo 3 donc par combinaisons : $x^3 - 13x^2 - 5x + 7 \equiv -1 - 13 + 5 + 7 \pmod 3$; c'est-à-dire : $x^4 - 13x^3 - 7x^2 - 2x \equiv 1 \pmod 3$.
x n'est pas solution.

$$\boxed{S = \{3k+1 \,|\, k \in \mathbb{Z}\}}.$$

□

I.5.4 Utilisations des congruences

I.5.4.a Détermination de restes

Exercice I.5.14. ***Déterminer le reste de la division euclidienne de $7^{2\,002}$ par 9.***

Solution *On a : $7^1 \equiv 7 \pmod 9$; de plus : $7^2 = 49 = 9 \times 5 + 4$; donc : $7^2 \equiv 4 \pmod 9$; d'où : $7^3 \equiv 28 \pmod 9$; mais : $28 = 9 \times 3 + 1$; donc : $7^3 \equiv 1 \pmod 9$.*
De plus : $2\,002 = 3 \times 667 + 1$.
Donc : $\left(7^3\right)^{667} \equiv 1^{667} \pmod 9$; d'où : $7^{2\,001} \times 7 \equiv 1 \times 7 \pmod 9$; c'est-à-dire : $7^{2\,002} \equiv 7 \pmod 9$.
Or : $0 \leqslant 7 < 9$; donc le reste la division euclidienne de $7^{2\,002}$ par 9 est 7. □

Exercice I.5.15. ***Déterminer, suivant les valeurs de l'entier naturel n, le reste de la division euclidienne de 5^n par 3.***

Solution *On a : $5^1 \equiv 2 \pmod 3$ et $5^2 \equiv 1 \pmod 3$.*
Si $n = 2k$ ($k \in \mathbb{N}$), on a : $\left(5^2\right)^k \equiv 1^k \pmod 3$; donc : $5^n \equiv 1 \pmod 3$.
Le reste de la division de 5^n par 3 est 1.
Si $n = 2k+1$ ($k \in \mathbb{N}$), on a : $\left(5^2\right)^k \times 5 \equiv 1^k \times 5 \pmod 3$; donc : $5^n \equiv 5 \pmod 3$; d'où : $5^n \equiv 2 \pmod 3$.
Le reste de la division de 5^n par 3 est 2. □

I.5.4.b Démonstration de propriétés

Exercice I.5.16. ***Soit n un entier naturel. Démontrer que $n\left(n^4-1\right)$ est multiple de 5.***

Solution *Cinq cas sont envisageables :*
$n \equiv 0 \pmod 5$; $n \equiv 1 \pmod 5$; $\cdots$; $n \equiv 4 \pmod 5$.
Les résultats sont regroupés dans le tableau ci-contre.
On en déduit que $n\left(n^4-1\right)$ est multiple de 5.

$n \equiv$	0	1	2	3	4
$\left(n^4-1\right) \equiv$	4	0	0	0	0
$n\left(n^4-1\right) \equiv$	0	0	0	0	0

□

Exercice I.5.17. ***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.

Solution ***1.*** *Huit cas sont envisageables :*
$n \equiv 0 \pmod 8$; $n \equiv 1 \pmod 8$; $\cdots$; $n \equiv 7 \pmod 8$.
Les résultats sont regroupés dans le tableau ci-contre.
On en déduit que le reste de la division euclidienne de n^2 par 8 est 0, 1 ou 4.

$n \equiv$	0	1	2	3	4	5	6	7
$n^2 \equiv$	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

Le reste ne vaut jamais 7, donc les nombres de la forme $8k+7$ ne sont jamais la somme de trois carrés parfaits. □

I.5.4.c Congruences particulières

Les critères de divisibilité par 2, 3, 4 ,5 9 et parfois 11, ont été utilisés au collège. Nous allons généraliser et démontrer ces propriétés à l'aide des congruences.
Dans cette partie, x désigne un entier naturel non nul et $\overline{a_n a_{n-1}\dots a_0}$ avec $a_n \neq 0$ son écriture décimale. On a : $x = a_n 10^n + a_{n-1}10^{n-1} + \dots + a_1 10^1 + a_0$.

Exercice I.5.18. ***(Congruences modulo 5)***

1. Vérifier que : $\forall p \in \mathbb{N}^*$, $10^p \equiv 0 \pmod 5$.
2. a. En déduire que : $x \equiv a_0 \pmod 5$.
b. Application
Déterminer le reste de la division euclidienne par 5 de 1 738, 2 352, 13 325 et 32 064 512.

Solution ***1.*** *Soit p un élément de $\mathbb{N}^*$, on a : $10^p = 5(2\times 10^{p-1})$ et $2\times 10^{p-1} \in \mathbb{Z}$; donc : $10^p \equiv 0 \pmod 5$.*

2. a. *On a : $x = a_0 + \sum_{p=1}^{n} a_p 10^p$ et $\sum_{p=1}^{n} a_p 10^p$ est une somme de multiple de 5, donc $\sum_{p=1}^{n} a_p 10^p$ est multiple de 5 ; d'où : $x \equiv a_0 \pmod 5$.*
b. Application
Les restes de la division euclidienne par 5 de 1 738, 2 352, 13 325 et 32 064 512 sont respectivement les mêmes restes que pour 8, 2, 5, 2 ; ces reste sont donc respectivement 3, 2, 0 et 2. □

Remarque En utilisant la congruence modulo 2, on établit de même que : $x \equiv a_0 \pmod 2$.

Exercice I.5.19. ***(Congruences modulo 4)***

1. Vérifier que : $\forall p \in \mathbb{N}\setminus\{0;1\}$, $10^p \equiv 0 \pmod 4$.
2. a. En déduire que : $x \equiv \overline{a_1 a_0} \pmod 4$.
b. Application
Déterminer le reste de la division euclidienne par 4 de 1 738, 2 352, 13 325 et 32 064 512.

Solution ***1.*** *Soit p un élément de $\mathbb{N}\setminus\{0;1\}$, on a : $10^p = 4(25\times 10^{p-2})$ et $25\times 10^{p-2} \in \mathbb{Z}$; donc : $10^p \equiv 0 \pmod 4$.*

2. a. *$x = \overline{a_1 a_0} + \sum_{p=2}^{n} a_p 10^p$ et $\sum_{p=2}^{n} a_p 10^p \in 4\mathbb{Z}$; donc : $x \equiv \overline{a_1 a_0} \pmod 4$.*
b. Application
Les restes de la division euclidienne par 4 de 1 738, 2 352, 13 325 et 32 064 512 sont respectivement les mêmes restes que pour 38, 52, 25, 12 ; ces reste sont donc respectivement 2, 0, 1 et 0. □

Remarque En utilisant la congruence modulo 25, on établit de même que : $x \equiv \overline{a_1 a_0} \pmod{25}$.

Exercice I.5.20. ***(Congruences modulo 9)***

1. Vérifier que : $\forall p \in \mathbb{N}$, $10^p \equiv 1 \pmod 9$.
2. a. En déduire que : $x \equiv \sum_{p=0}^{n} a_p \pmod 9$.
b. Application
Déterminer le reste de la division euclidienne par 9 de 1 738, 2 352, 13 325 et 32 064 512.

Solution 1. *Soit p un élément de $\mathbb{N}$.*
Si $p=0$, on a : $10^0=1$; donc : $10^p\equiv 1\,(\text{mod}\,9)$.
Si $p\neq 0$, on a : $10^p-1^p=(10-1)(10^{p-1}\times 1^0+10^{p-2}\times 1^1+\cdots+10^1\times 1^{p-2}+10^0\times 1^{p-1})$; donc : $10^p\equiv 1\,(\text{mod}\,9)$.
2. a. *On a : $x=a_n10^n+a_{n-1}10^{n-1}+\ldots+a_110^1+a_0$ et $\forall p\in\mathbb{N},\ a_p10^p\equiv a_p\,(\text{mod}\,9)$;*
donc par somme : $x\equiv\sum_{p=0}^{n}a_p\,(\text{mod}\,9)$.

b. Application
On a : $1738\equiv 1+7+3+8\,(\text{mod}\,9)$ et $1+7+3+8=19=2\times 9+1$; donc le reste de la division de 1 738 par 9 est 1. De même, les restes de la division par 9 de 2 352, 13 325 et 32 064 512 sont respectivement 3, 5 et 5. □

Remarque En utilisant la congruence modulo 3, on établit de même que : $x\equiv\sum_{p=0}^{n}a_p\,(\text{mod}\,3)$.

Exercice I.5.21. ***(Congruences modulo 11)***

1. Vérifier que : $\forall p\in\mathbb{N},\ 10^p\equiv(-1)^p\,(\text{mod}\,11)$.

2. a. En déduire que : $x\equiv\sum_{p=0}^{n}(-1)^pa_p\,(\text{mod}\,11)$.

b. Application

Déterminer le reste de la division euclidienne par 11 de 1 738, 2 352, 13 325 et 32 064 512.

Solution 1. *Soit p un élément de $\mathbb{N}$.*
Si $p=0$, on a : $10^p=1$ et $(-1)^p=1$; donc : $10^p\equiv(-1)^p\,(\text{mod}\,11)$.
Si $p\neq 0$, on a : $10\equiv -1\,(\text{mod}\,11)$; donc : $10^p\equiv(-1)^p\,(\text{mod}\,11)$.
2. a. *On a : $x=a_n10^n+a_{n-1}10^{n-1}+\ldots+a_110^1+a_0$ et $\forall p\in\mathbb{N},\ a_p10^p\equiv(-1)^pa_p\,(\text{mod}\,11)$;*
donc par somme : $x\equiv\sum_{p=0}^{n}(-1)^pa_p\,(\text{mod}\,11)$.

b. Application
On a : $1738\equiv -1+7-3+8\,(\text{mod}\,11)$; donc le reste de la division euclidienne de 1 738 par 11 est 0. De même, les restes de la division euclidienne par 11 de 2 352, 13 325 et 32 064 512 sont respectivement 9, 4 et 7. □

I.5.4.d Autour du théorème chinois

Exercice I.5.22. ***(Centres étrangers groupe I – 2001)***

Un astronome a observé au jour J_0 la corps céleste A, qui apparaît périodiquement tous les 105 jours. Six jours plus tard (J_0+6), il observe le corps B, dont la période d'apparition est de 81 jours. On appelle J_1 le jour de la prochaine apparition simultanée des deux objets aux yeux de l'astronome.
Le but de cet exercice est de déterminer la date de ce jour J_1.

1. Soient u et v le nombre de périodes effectuées respectivement par A et B entre J_0 et J_1.
Montrer que le couple (u,v) est solution de l'équation :

$$\mathbf{35}x-\mathbf{27}y=\mathbf{2}\qquad(E_1)$$

2. a. Déterminer un couple d'entiers relatifs (x_0,y_0) solution particulière de l'équation :

$$\mathbf{35}x-\mathbf{27}y=\mathbf{1}\qquad(E_2)$$

b. En déduire une solution particulière (u_0,v_0) de (E_1).

c. Déterminer toutes les solutions de (E_1).

d. Déterminer la solution (u,v) permettant de déterminer J_1.

3. a. Combien de jours s'écouleront entre J_0 et J_1 ?

b. Le jour J_0 était le 7 décembre 1999, quelle est la date exacte du jour J_1 ? (l'année 2000 était bissextile).

c. Si l'astronome manque ce futur rendez-vous, combien de jour devra-t-il attendre jusqu'à la prochaine conjonction des deux astres ?

Solution 1. *Soit Δ le nombre de jours qui s'écoulent entre J_0 et J_1. u est le nombre de périodes de A entre J_0 et J_1, donc : $\Delta = 105u$.*
De même : $\Delta - 6 = 81v$; donc : $105u = \Delta = 81v + 6$; d'où, en divisant par 3 :

$$35u - 27v = 2.$$

(u, v) *est solution de* (E_1)

2. a. *Appliquons l'algorithme d'*EUCLIDE *au couple $(35;27)$.*
On a : $35 = 27 + 8$; $27 = 3 \times 8 + 3$; $8 = 3 \times 3 - 1$. On en déduit que :

27 *et* 35 *sont premiers entre eux.*

De plus : $1 = 3 \times 3 - 8 = 3(27 - 3 \times 8) - 8 = 3 \times 2710 \times 8 = 3 \times 27 - 10(35 - 27) = 35 \times (-10) - 27 \times (-13)$.
On peut donc prendre :

$$\boxed{(x_0, y_0) = (-10; -13)}.$$

b. *En multipliant membre à membre l'égalité précédente, il vient :*

$$35 \times (-20) - 27 \times (-26) = 2.$$

On peut donc prendre :

$$\boxed{(u_0, v_0) = (-20; -26)}.$$

c. *Soit (x, y) une solution de (E_1). On a : $35x - 27y = 2 = 35 \times (-20) - 27 \times (-26)$; donc :*

$$35(x + 20) = 27(y + 26) \tag{I.7}$$

27 divise $35(x + 20)$ et, d'après ***2.a.*** *est premier avec 35, donc, d'après le théorème de* GAUSS*, 27 divise $x + 20$. Désignons par k le quotient, on a donc : $x + 20 = 27k$ et $x = 27k - 20$.*
En remplaçant $(x + 20)$ par $27k$ dans (I.7), il vient : $27(y + 26) = 35 \times 27k$ d'où l'on tire : $y = 35k - 26$.
On en déduit que toutes les solutions de (E_1) sont de la forme : $(27k - 20; 35k - 26)$ avec $k \in \mathbb{Z}$.

Réciproquement, vérifions que tout couple de cette forme est solution de (E_1).
Pour tout entier k, on a : $35(27k - 20) - 27(35k - 26) = -35 \times 20 + 27 \times 26 = 702 - 700 = 2$; donc :

$$\boxed{S_{(E_1)} = \{(27k - 20; 35k - 26) \mid k \in \mathbb{Z}\}}.$$

d. *La valeur de k permettant de déterminer J_1 est la valeur pour laquelle les entiers : $u = 27k - 20$ et $v = 35k - 26$; sont des entiers naturels les plus petits possibles on déduit que $k = 1$ et que :*

$$\boxed{(u; v) = (7; 9)}.$$

3. a. *On a : $\Delta = 105u$ et $u = 7$; donc : $\Delta = 735$.*

Il s'écoule 735 *jours entre* J_0 *et* J_1.

b. *Entre le 7 décembre 1999 et le 7 décembre 2001 il s'écoule deux ans (dont une année bissextile), c'est-à-dire : $365 + 366 = 731$ jours. J_1 est donc 4 jours après le 7 décembre 2001.*

J_1 *est le 11 décembre 2001.*

c. *Deux méthodes sont envisageables.*

1re méthode

La prochaine conjonction aura lieu PPCM(105;81) *jours après* J_1.
PPCM(105;81) = 3 PPCM(35;27) = $3\times35\times27 = 2835$ *(car on a vu en* ***2.a.*** *que* 27 *et* 35 *sont premiers entre eux.)*

Si l'astronome manque le rendez-vous, il devra patienter 2 835 jours jusqu'à la prochaine conjonction des deux astres.

2e méthode

Soit J_2 *la date de la conjonction suivante.*
Cette conjonction aura lieu pour $k = 2$ *et on aura donc :* $(u;v) = (34;44)$ *en passant de* J_1 *à* J_2*, on a :* $\Delta u = 34-7 = 27$. *Il s'écoule 27 périodes de A (*105 *jours) entre* J_1 *et* J_2.

Si l'astronome manque le rendez-vous, il devra patienter 2 835 jours jusqu'à la prochaine conjonction des deux astres.

□

Exercice I.5.23. ***(Théorème chinois)***

Soit m et n deux entiers naturels non nuls, δ leur PGCD et μ leur PPCM.

1. Démontrer que pour tous entiers a et b, on a :

$$\begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases} \iff a \equiv b \pmod{\mu} \tag{I.8}$$

2. Soit α, β deux entiers. On se propose de résoudre le système :

$$\begin{cases} x \equiv \alpha \pmod{m} \\ x \equiv \beta \pmod{n} \end{cases} \tag{I.9}$$

Démontrer que si $\beta-\alpha$ n'est pas multiple de δ, alors le système n'a pas de solution.

3. On suppose désormais que α et β sont multiples de δ et on désigne par α' et β' leurs quotients respectifs par δ.

a. Justifier l'existence d'un couple d'entiers (u,v) tels que : $mu+nv=\delta$.

b. Justifier que : $\begin{cases} mu \equiv 0 \pmod{m} \\ mu \equiv \delta \pmod{n} \end{cases}$ ***et*** $\begin{cases} nv \equiv \delta \pmod{m} \\ nv \equiv 0 \pmod{n} \end{cases}$.

c. En déduire que $\beta' mu + \alpha' nv$ est une solution particulière de l'équation (I.9).

4. Résoudre l'équation (I.9).

5. Application : utiliser le résultat obtenu et un tableur pour retrouver les résultats obtenus en 3.b et 3.c de l'exercice Centres étrangers groupe I – 2001 (exercice I.5.22.).

Solution 1. *Soit a et b deux entiers relatifs.*

Supposons que : $\begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases}$ *; démontrons que :* $a \equiv b \pmod{\mu}$.

$b-a$ *est multiple de m et n, donc de leur* PPCM *; d'où :* $a \equiv b \pmod{\mu}$.

Réciproquement, supposons que : $a \equiv b \pmod{\mu}$ *; démontrons que :* $\begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases}$.

$b-a$ *est multiple de* μ *et* μ *est multiple de m et n donc, par transitivité, $b-a$ est multiple de m et n. On en déduit que :* $\begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases}$.

L'équivalence (I.8) *est donc vérifiée pour tous couples (a,b) d'entiers naturels.*

2. *On doit démontrer une implication entre deux négations.*
Par contraposée, il suffit de démontrer que si le système a au moins une solution alors $\beta-\alpha$ est multiple de δ. Supposons donc que le système a une solution (au moins) x. Il existe alors deux

entiers a et b tels que : $\alpha + am = x = \beta + bn$; d'où l'on tire : $\beta - \alpha = bn - am$.
m et n sont multiples de δ, donc $bn - am$ aussi.
Si $\beta - \alpha$ n'est pas multiple de δ, alors le système n'a pas de solution.

3. a. *On sait que les nombre de la forme : $mu + nv$; sont les multiples de δ, il existe donc un couple d'entiers (u, v) tel que :*

$$mu + nv = \delta.$$

b. *mu est multiple de m donc : $mu \equiv 0 \,(\text{mod}\, m)$. d'après **2.a.**, $mu - \delta$ est multiple de n, donc : $mu \equiv \delta \,(\text{mod}\, n)$. On établi de même que :* $\begin{cases} nv \equiv \delta \,(\text{mod}\, m) \\ nv \equiv 0 \,(\text{mod}\, n) \end{cases}$.

c. *Par produits par α' et par β', on en déduit que :* $\begin{cases} \beta' mu \equiv 0 \,(\text{mod}\, m) \\ \beta' mu \equiv \beta \,(\text{mod}\, n) \end{cases}$ *et* $\begin{cases} \alpha' nv \equiv \alpha \,(\text{mod}\, m) \\ \alpha' nv \equiv 0 \,(\text{mod}\, n) \end{cases}$;
puis par sommes, il vient :

$$\begin{cases} \beta' mu + \alpha' nv \equiv \alpha \,(\text{mod}\, m) \\ \beta' mu + \alpha' nv \equiv \beta \,(\text{mod}\, n) \end{cases}.$$

Donc $\beta' mu + \alpha' nv$ est une solution particulière de l'équation (I.9).

4. *On déduit de **3.c.** et de **1.** que :*

$$(\text{I.9}) \iff \begin{cases} x \equiv \alpha' mu + \beta' nv \,(\text{mod}\, m) \\ x \equiv \alpha' mu + \beta' nv \,(\text{mod}\, n) \end{cases} \iff x \equiv \alpha' mu + \beta' nv \,(\text{mod}\, \mu).$$

D'où il vient l'ensemble des solutions de (I.9) :

$$S = \{ \alpha' mu + \beta' nv + k\mu \mid k \in \mathbb{Z} \} \tag{I.10}$$

5. Application
Prenons comme unité de temps le jour et comme origine des temps J_0.
L'astronome a observé au jour J_0 la corps céleste A, qui apparaît périodiquement tous les 105 jours ; donc les jours d'apparition de l'astre A sont les solutions de l'équation :

$$J \equiv 0 \,(\text{mod}\, 105).$$

Six jours plus tard ($J_0 + 6$), il observe le corps B, dont la période d'apparition est de 81 jours ; donc les jours d'apparition de l'astre B sont les solutions de l'équation :

$$J \equiv 6 \,(\text{mod}\, 81).$$

Les jours d'apparitions simultanées des deux astres sont donc les solutions du système :

$$\begin{cases} J \equiv 0 \,(\text{mod}\, 105) \\ J \equiv 6 \,(\text{mod}\, 81) \end{cases}. \tag{I.11}$$

On a donc : $(m; n) = (105; 81)$; $(\delta; \mu) = (3; 2\,835)$; $(\alpha; \beta) = (0; 6)$; $(\alpha'; \beta') = (0; 2)$.
De plus : $-10 \times 105 + 13 \times 81 = 3$; on peut donc prendre : $(u; v) = (-10; 13)$; on aura alors : $\alpha' mu + \beta' nv = 2\,106$. Les solutions du systèmes sont donc les nombres de la forme : $2\,106 + 2\,835k$ avec $k \in \mathbb{Z}$. □

Le théorème chinois est le théorème qui affirme que les solutions de (I.9) est donné par (I.10). Ce théorème, connu des Chinois depuis la Haute Antiquité, était utilisé pour déterminer les jours où deux astres sont en conjonction. De nos jours, il intervient dans des algorithmes permettant à un ordinateur de coder des nombres qui s'écrivent, en numération décimale, avec plus de chiffres qu'autorise la capacité de la machine.

I.5.5 Exercices

I.5.a. Démontrer que : $2^{27} \equiv 3 \pmod 5$

I.5.b. Démontrer, en utilisant les congruences, que pour tout entier naturel n : $2^{4n} - 2^n$ est multiple de 7.

I.5.c. Démontrer, sans utiliser les congruences, que pour tout entier naturel n : $2^{4n} - 2^n$ est multiple de 7.

I.5.d. Soit n et d deux entiers naturels non nuls tels que d divise n. Démontrer que pour tous entiers relatifs a et b on a :
$a \equiv b \pmod n \quad \Longrightarrow \quad a \equiv b \pmod d$.

I.5.e. Sans effectuer de division euclidienne, vérifier que 43 758 est divisible par 99.

I.5.f. Démontrer que la somme des cubes de trois entiers relatifs consécutifs est divisible par 9.

Index

$n\mathbb{Z}$, 12

base de numération, 9

congruence, 28–41

diviseur, 13
    propre, 13

multiple, 11

nombre
    composé, 15, 41
    premier, 15, 41

PGCD, 20
PPCM, 19

relation d'ordre, 6

système
    binaire, 9, 10
    hexadécimal, 9, 10
    sexagésimal, 9