# Arithmétique

# Table des matières

T	Divisibilite dans $\mathbb{Z}$	1
<b>2</b>	Relations d'équivalence et ensemble quotient	15

3 Congruences et  $\mathbb{Z}/_{n\mathbb{Z}}$ 

# 1 Divisibilité dans $\mathbb{Z}$

Dans ce paragraphe nous présentons les propriétés de la division dans l'ensemble des entiers relatifs, ainsi que le pgcd et le ppcm. Nous établissons les deux théorèmes fondamentaux de Gauss et de Bézout et nous faisons quelques rappels sur les nombres premiers.

## 1.1 Nombres premiers

On appelle entier naturel tout élément de

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

On appelle entier relatif tout élément de

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

#### Définitions 1.

On dit qu'un entier relatif a est un multiple d'un entier relatif b lorsqu'il existe un entier relatif k tel que a = kb.

Pour tout  $a \in \mathbb{Z}$  l'ensemble des multiples de a se note  $a\mathbb{Z}$ , *i.e.*  $a\mathbb{Z} = \{an \mid n \in \mathbb{Z}\}.$ 

On dit qu'un entier relatif non nul b est un diviseur de a, lorsqu'il existe un entier relatif k tel que a = kb. Cela se note b|a (lire « b divise a »).

Exemples 1.  $\diamond$  L'entier 3 possède exactement quatre diviseurs : -3, -1, 1 et 3.

 $\diamond$  Nous avons  $5\mathbb{Z} = \{5k \mid k \in \mathbb{Z}\} = \{\ldots, -20, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}.$ 

#### Proposition 1.2

Pour tous a, b et c dans  $\mathbb{Z} \setminus \{0\}$  nous avons les propriétés suivantes :

- $\diamond a|a, \pm 1|a \text{ et } a|0;$
- $\diamond$  si a|b et b|c, alors a|c;
- $\diamond$  si a|b et si  $b \neq 0$ , alors  $|a| \leq |b|$ ;
- $\diamond$  si a|b et b|a, alors  $a=\pm b$ ;
- $\diamond$  si a|b et a|c, alors  $a|(kb+\ell c)$  quels que soient les entiers  $k, \ell \in \mathbb{Z}$ . En particulier, a|b+c et a|b-c.

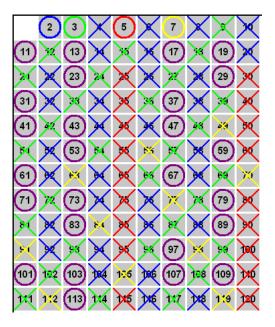
Démonstration.  $\diamond$  Cela découle du fait que  $a=1\times a=(-1)\times (-a)$  et  $0=0\times a$ .

- $\diamond$  Si a|b et b|c, alors il existe des entiers q et r tels que b=aq et c=br. Nous en déduisons que c=aqr=a(qr) donc a|c.
- $\diamond$  Supposons que a|b, c'est-à-dire b=aq avec  $q\in\mathbb{Z}$ . Si  $b\neq 0$ , alors  $q\neq 0$  donc  $|q|\geq 1$ . Par suite  $|b|=|a||q|\geq |a|$ .
- $\diamond$  Supposons que a|b et que b|a; autrement dit il existe des entiers q et r tels que a=bq et b=ar. Nous avons a=bq=arq qui comme a est non nul conduit à 1=rq. Puisque r et q sont des entiers,  $r=q=\pm 1$  et  $a=\pm b$ .
- $\diamond$  Supposons que a divise b et c. Il existe alors des entiers p et q tels que b=ap et c=aq. Pour tous entiers k et  $\ell$  nous avons  $kb+\ell c=a(kp+\ell q)$  donc  $a|(kb+\ell c)$ .

#### Définition 1.3

Un entier p > 2 est premier lorsqu'il possède pour seuls diviseurs positifs 1 et lui-même.

Le crible d'Eratosthène est un procédé qui permet de trouver tous les nombres premiers inférieurs à un certain entier naturel donné N. Nous procédons par élimination : nous supprimons d'une table des entiers de 2 à N tous les multiples d'un entier (autre que lui-même). En supprimant tous ces multiples il ne reste à la fin que les entiers qui ne sont multiples d'aucun entier à part 1 et eux-mêmes et qui sont donc les nombres premiers. Autrement dit nous commençons par rayer les multiples de 2 mais pas 2, les multiples de 3 mais pas 3, les multiples de 5 mais pas 5... On peut s'arrêter lorsque le carré du plus petit entier restant est supérieur au plus grand entier restant (tous les non premiers ont déjà été rayés précédemment). Finalement tous les entiers non rayés sont les nombres premiers inférieurs à N.



Exemples 2.  $\diamond$  1 n'est pas premier et 2 est le seul nombre premier pair.

- $\diamond$  101 et 103 sont premiers.
- $\diamond$  91 n'est pas premier : 91 = 7 × 13.

#### Proposition 1.4

Soit  $n \ge 2$  un entier. Le plus petit diviseur positif d de n tel que d > 1 est un nombre premier.

Démonstration. Soit D l'ensemble des diviseurs de n. D'une part  $D \neq \emptyset$  (car n appartient à D), d'autre part  $D \subset \{2, 3, ..., n\}$ . Soit  $p = \min D$ ; alors p est premier. En effet, sinon il existe 1 < q < p tel que q|p; or p|n donc q|n: contradiction avec le fait que  $p = \min D$ .

## Théorème 1.5

Il existe une infinité de nombres premiers.

Démonstration. Soit un entier  $n \geq 2$ . Alors l'entier N = n! + 1 n'a aucun diviseur compris entre 2 et n; en effet si N possédait un diviseur k compris entre 2 et n alors k diviserait n! et N donc diviserait N - n! = 1 ce qui n'est pas possible. Or N possède au moins un diviseur premier p (Proposition 1.4). Puisque  $p \geq 2$ , nous en déduisons que p > n. Cela montre qu'il existe des nombres premiers aussi grands que l'on veut d'où une infinité.

#### Proposition 1.6

Tout entier n > 1 est premier ou produit de nombres premiers.

Démonstration. Soit un entier n > 1. Nous raisonnons par récurrence : 2 est premier. Supposons que tout 1 < a < n est un nombre premier ou un produit de nombres premiers. Si n n'est pas premier, il se factorise en n = pq, où les entiers p et q satisfont les inégalités 1 et <math>1 < q < n. Par hypothèse de récurrence les entiers p et q sont produits de nombres premiers, il en résulte que n aussi.

#### 1.2 Division euclidienne

#### Proposition-Définition 1.7

Soit b un élément de  $\mathbb{Z} \setminus \{0\}$ . Pour tout  $a \in \mathbb{Z}$  il existe  $q \in \mathbb{Z}$  et  $r \in \mathbb{Z}$  uniques tels que a = bq + r et  $0 \le r < |b|$ .

L'entier q s'appelle le quotient de la division euclidienne de a par b et l'entier r s'appelle le reste de la division euclidienne de a par b.

Remarques 1.  $\diamond$  Nous avons l'équivalence suivante : b divise a si et seulement si le reste de la division de a par b est nul.

 $\diamond$  Si b > 0, alors le quotient q est l'unique entier tel que  $q \leq \frac{a}{b} < q+1$ : c'est la partie entière du nombre rationnel  $\frac{a}{b}$ .

Démonstration. Supposons dans un premier temps que b > 0. Soit E l'ensemble des multiples de b inférieurs ou égaux à a. Remarquons que E est une partie de  $\mathbb{Z}$  non vide  $(b \in E)$  majorée par a; il en résulte que E a un plus grand élément que nous écrirons bq. Le multiple b(q+1) n'appartient alors pas à E. Ainsi  $bq \le a < b(q+1)$ . En posant r = a - bq il vient  $0 \le r < b(q+1) - bq = b$  et a = bq + r.

Supposons désormais que b < 0. Appliquons ce qui précède à a et -b: il existe q et r dans  $\mathbb{Z}$  tels que a = (-b)q + r et  $0 \le r < -b$  donc a = b(-q) + r et  $0 \le r < |b|$ .

Montrons maintenant que le couple (q,r) est unique. Raisonnons par l'absurde : supposons que le couple (q,r) n'est pas unique. Soient (q,r) et (q',r') tels que a=bq+r=bq'+r' avec  $0 \le r < |b|$  et  $0 \le r' < |b|$ . Par soustraction il vient 0 = b(q-q') + (r-r') d'où

$$|b||q - q'| = |r - r'|.$$

Mais comme r et r' sont compris entre 0 et |b|-1 nous avons |r-r'|<|b| d'où |b||q-q'|<|b|. Puisque |b|>0, nous en déduisons que |q-q'|<1 et comme |q-q'| est un entier positif ou nul il s'ensuit |q-q'|=0, ou encore q=q'. Par conséquent r=r'.

Exemples 3. Voici des divisions euclidiennes :

- $\diamond$  division de 12 par 5 :  $12 = 5 \times 2 + 2$ ;
- $\diamond$  division de 12 par  $-5: 12 = (-5) \times (-2) + 2;$
- ♦ division de -12 par  $5: -12 = 5 \times (-3) + 3$ ;
- $\diamond$  division de -12 par  $-5: -12 = (-5) \times 3 + 3$ .

# 1.2.1 Une application : les sous-groupes de $\mathbb{Z}$

#### Définition 1.8

Un sous-ensemble G de  $\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$  si

- $\diamond G \neq \emptyset$ :
- $\diamond$  si g et h appartiennent à G, alors g + h appartient à G;
- $\diamond$  si g appartient à G, alors -g appartient à G.

Exemple 4. Pour tout  $k \in \mathbb{N}$ , l'ensemble  $k\mathbb{Z} := \{kn \mid n \in \mathbb{Z}\}$  est un sous-groupe de  $(\mathbb{Z}, +)$ . En effet,

- $\diamond k\mathbb{Z} \neq \emptyset \text{ car } 0 \in k\mathbb{Z};$
- $\diamond$  soient g, h dans  $k\mathbb{Z}$ , alors g = kn avec  $n \in \mathbb{Z}$  et h = kn' avec  $n' \in \mathbb{Z}$ . Alors g + h s'écrit k(n + n') avec  $n + n' \in \mathbb{Z}$  d'où g + h appartient à  $k\mathbb{Z}$ ;
- $\diamond$  soit g dans  $k\mathbb{Z}$ ; alors g s'écrit kn avec  $n \in \mathbb{Z}$  et -g s'écrit k(-n) avec  $-n \in \mathbb{Z}$  d'où -g appartient à  $k\mathbb{Z}$ .

L'énoncé suivant assure que ce sont les seuls sous-groupes de  $(\mathbb{Z},+)$ :

#### Théorème 1.9

Soit G un sous-groupe de  $(\mathbb{Z},+)$ . Il existe un unique entier  $d \geq 0$  tel que  $G = d\mathbb{Z}$ .

 $D\acute{e}monstration.$   $\diamond$  Montrons tout d'abord l'existence de d.

Si  $G = \{0\}$ , alors  $G = 0\mathbb{Z}$ .

Supposons maintenant le sous-groupe G non trivial, i.e.  $G \neq \{0\}$ ; G possède alors un élément g non nul. Il possède même un élément strictement positif; en effet c'est clair si g > 0 et si g < 0 il suffit de prendre l'opposé (-g) de g. L'ensemble des éléments strictement positifs de G étant non vide, il possède un plus petit élément d. Nous allons montrer que  $G = d\mathbb{Z}$ .

Puisque G est un sous-groupe de  $\mathbb{Z}$  contenant d, il contient  $\{dn \mid n \in \mathbb{Z}\}$ , c'est-à-dire  $d\mathbb{Z}$ .

Reste à montrer l'inclusion réciproque  $G \subset d\mathbb{Z}$ . Soit  $g \in G$ . Comme d > 0 on peut effectuer la division euclidienne de g par d. Elle fournit un couple (q,r) d'entiers avec  $0 \le r < d$  tels que g = dq + r. Ainsi r = g - dq. Puisque  $d\mathbb{Z} \subset G$ , nous avons :  $-dq \in G$ . Étant donné que G est un sous-groupe g - dq appartient à G, i.e. r appartient à G. Puisque  $0 \le r < d$  et puisque d est le plus petit élément strictement positif de G, nous avons r = 0 et ainsi g = dq. En particulier, g appartient à  $d\mathbb{Z}$  et  $G \subset d\mathbb{Z}$ .

Les inclusions  $d\mathbb{Z} \subset G$  et  $G \subset d\mathbb{Z}$  conduisent à l'égalité  $G = d\mathbb{Z}$ .

♦ Il reste à s'assurer de l'unicité de d. Soit  $\delta > 0$  un entier tel que  $G = d\mathbb{Z} = \delta\mathbb{Z} = \{0\}$ . Si d = 0, alors  $G = 0\mathbb{Z}$  et  $\delta$  est donc nul puisque  $\delta$  appartient à  $\delta\mathbb{Z} = G$ . Supposons  $d \neq 0$ . Alors  $G \neq \{0\}$  et  $\delta \neq 0$ . D'une part comme d appartient à  $G = \delta\mathbb{Z}$  il existe  $a \in \mathbb{Z}$  tel que  $d = a\delta$ . D'autre part  $G = d\mathbb{Z}$  et  $\delta$  appartient à G; il existe donc  $b \in \mathbb{Z}$  tel que  $\delta = bd$ . Ainsi  $d = a\delta = abd$  soit d(1 - ab) = 0. Par hypothèse d est non nul donc 1 - ab = 0 soit ab = 1. Puisque a et b sont entiers ils sont ou bien tous deux égaux à 1 ou bien tous deux égaux à -1. Si a et b étaient tous deux égaux à -1, on aurait  $\delta = bd = -d$  ce qui est impossible car d et  $\delta$  sont strictement positifs. Par suite a = b = 1 et  $\delta = bd = d$ .

# 1.3 Pgcd

#### Définitions 1.10

Soient  $a, b \in \mathbb{Z}$  des entiers non nuls. Le plus grand entier qui divise a et b s'appelle le pgcd de a et b et se note pgcd(a, b) ou  $a \wedge b$ .

On dit que a et b sont premiers entre eux si pgcd(a, b) = 1.

On veillera à ne pas confondre les définitions de « nombre premier » et « nombres premiers entre eux ».

Exemple 5. Puisque les diviseurs communs de 20 et 30 sont 1, 2, 5 et 10 nous avons pgcd(20,30) = 10.

Remarques 2.  $\diamond$  Si a > 0, alors pgcd(a, 0) = a.

- $\diamond$  Pour tout  $a \in \mathbb{Z}$ ,  $\operatorname{pgcd}(a, 1) = 1$ .
- $\diamond$  Si a divise b, alors  $\operatorname{pgcd}(a,b) = |a|$ .

#### Proposition 1.11

Soit p un nombre premier. Pour tout entier  $n \in \mathbb{Z}$  nous avons

$$pgcd(n, p) = \begin{cases} 1 \text{ si } p \text{ ne divise pas } n \\ p \text{ si } p \text{ divise } n \end{cases}$$

Démonstration. Tout diviseur positif commun à n et p est égal à 1 ou à p.

#### Proposition 1.12

Pour tous entiers a et b strictement positifs, nous avons  $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(b,r)$  où r est le reste de la division euclidienne de a par b.

Démonstration. Si d divise a et b, alors d divise a et bq; par conséquent d divise a - bq = r. Réciproquement, si d divise b et r, alors d divise bq et r; il en résulte que d divise bq + r = a. L'ensemble des diviseurs communs à a et b est donc l'ensemble des diviseurs communs à b et c.

## 1.3.1 Calcul du pgcd : l'algorithme d'Euclide

Nous exploitons la Proposition 1.12 pour calculer le pgcd. Soient a et b des entiers positifs. Faisons les divisions successives :

$$a = bq_1 + r_1$$

$$b = r_1q_2 + r_2$$

$$r_1 = r_2q_3 + r_3$$

$$\vdots \quad \vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n$$

$$r_{n-1} = r_nq_{n+1} + 0$$

où 
$$0 = r_{n+1} < r_n < \ldots < r_2 < r_1 < |b|$$
.

Puisque les restes sont positifs ou nuls et diminuent strictement le dernier est nul. Le dernier reste non nul est un nombre  $r_n > 0$  tel que  $r_n$  divise  $r_{n-1}$ ; ainsi

$$pgcd(a, b) = pgcd(b, r_1) = pgcd(r_1, r_2) = \dots = pgcd(r_{n-1}, r_n) = r_n$$

Cette méthode de calcul du pgcd s'appelle l'algorithme d'Euclide.

#### Proposition 1.13

Soient a et b deux entiers strictement positifs. pgcd(a, b) est le dernier reste non nul dans la suite des divisions de l'algorithme d'Euclide.

Exemple 6. Déterminons pgcd(137, 24).

Nous avons les divisions euclidiennes successives suivantes :

$$137 = 5 \times 24 + 17$$

$$24 = 1 \times 17 + 7$$

$$17 = 2 \times 7 + 3$$

$$7 = 2 \times 3 + 1$$

$$3 = 3 \times 1 + 0$$

Il s'en suit que pgcd(137, 24) = 1.

Exemple 7. Les calculs ci-dessus montrent que 137 et 24 sont premiers entre eux.

Exemple 8. Déterminons pgcd(931, 513). Nous avons les divisions euclidiennes successives suivantes :

$$931 = 513 \times 1 + 418$$

$$513 = 418 \times 1 + 95$$

$$418 = 95 \times 4 + 38$$

$$95 = 38 \times 2 + 19$$

$$38 = 19 \times 2 + 0$$

Il s'en suit que pgcd(931, 513) = 19.

#### 1.3.2 Les théorèmes de Bézout et de Gauss

# Théorème 1.14: (Bézout)

Soient  $a, b \in \mathbb{Z}$  des entiers non tous deux nuls. Alors il existe  $u, v \in \mathbb{Z}$  tels que  $au + bv = \operatorname{pgcd}(a, b)$ ; on parle de relation de Bézout.

 $D\acute{e}monstration$ . Nous pouvons supposer a et b positifs. Notons D l'ensemble des entiers de la forme au' + bv' où u', v' appartiennent à  $\mathbb{Z}$ :

$$D = \{ au' + bv' \, | \, u', \, v' \in \mathbb{Z} \}.$$

Si des entiers n et m appartiennent à D, alors le reste de la division de n par m s'écrit n-qm avec  $q \in \mathbb{Z}$ , donc appartient aussi à D. Comme a, b appartiennent à D, nous constatons que dans l'algorithme d'Euclide tous les restes sont des éléments de D; en particulier,  $\operatorname{pgcd}(a,b)$  appartient à D.

# Méthode pour trouver une relation de Bézout.

Exemple 9. L'exemple précédent assure l'existence d'entiers u et v tels que 931u + 513v = 19. Voici comment calculer explicitement u et v:

$$931 = 513 \times 1 + 418 \iff \begin{pmatrix} 513 \\ 418 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 931 \\ 513 \end{pmatrix}$$

$$513 = 418 \times 1 + 95 \iff \begin{pmatrix} 418 \\ 95 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 513 \\ 418 \end{pmatrix}$$

$$418 = 95 \times 4 + 38 \iff \begin{pmatrix} 95 \\ 38 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 418 \\ 95 \end{pmatrix}$$

$$95 = 38 \times 2 + 19 \iff \begin{pmatrix} 38 \\ 19 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 95 \\ 38 \end{pmatrix}$$

Il en résulte que

version équation :

$$\begin{array}{rll} 19 & = & 95 - 38 \times 2 \\ 19 & = & 95 - (418 - 95 \times 4) \times 2 = -418 \times 2 + 95 \times 9 \\ 19 & = & -418 \times 2 + (513 - 418) \times 9 = 513 \times 9 - 418 \times 11 \\ 19 & = & 513 \times 9 - (931 - 513 \times 1) \times 11 = -11 \times 931 + 20 \times 513. \end{array}$$

♦ version matricielle : On peut utiliser le calcul matriciel pour écrire les divisions euclidiennes :

$$a = bq + r \Longleftrightarrow \begin{pmatrix} b \\ r \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

$$\begin{pmatrix} 38 \\ 19 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 931 \\ 513 \end{pmatrix}$$
$$= \begin{pmatrix} 5 & -9 \\ -11 & 20 \end{pmatrix} \begin{pmatrix} 931 \\ 513 \end{pmatrix}$$

et en calculant la seconde ligne du produit matriciel de droite nous obtenons la relation de Bézout souhaitée :  $19 = -11 \times 931 + 20 \times 513$ .

**Notations**. Rappelons que pour tout entier a nous notons  $a\mathbb{Z}$  l'ensemble des multiples de a. Si a et b sont des entiers, nous notons  $a\mathbb{Z} + b\mathbb{Z}$  l'ensemble des entiers de la forme au + bv où u, v appartiennent à  $\mathbb{Z}$ .

#### Corollaire 1.15

Soient a et b des entiers non tous deux nuls.

- 1. Nous avons l'égalité :  $a\mathbb{Z} + b\mathbb{Z} = \operatorname{pgcd}(a, b)\mathbb{Z}$ .
- 2. Nous avons les équivalences :

a et b sont premiers entre eux  $\iff$   $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$   $\iff$  il existe des entiers  $u, v \in \mathbb{Z}$  tels que au + bv = 1

3. Les diviseurs communs à a et b sont les diviseurs de pgcd(a,b):

$$\forall n \in \mathbb{Z}, (n|a \text{ et } n|b) \iff n|\operatorname{pgcd}(a,b).$$

- 4. Pour tout entier  $k \neq 0$ , nous avons :  $\operatorname{pgcd}(ka, kb) = |k| \operatorname{pgcd}(a, b)$ .
- 5. Les entiers  $a' = \frac{a}{\operatorname{pgcd}(a,b)}$  et  $b' = \frac{b}{\operatorname{pgcd}(a,b)}$  sont premiers entre eux.

Démonstration. Posons d = pgcd(a, b).

- 1. Le théorème de Bézout assure que d appartient à  $a\mathbb{Z} + b\mathbb{Z}$ , d'où  $d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$ . Réciproquement, a et b sont multiples de d, donc tout entier  $ak + b\ell \in a\mathbb{Z} + b\mathbb{Z}$  est multiple de d c'est-à-dire appartient à  $d\mathbb{Z}$ .
- 2. Résulte de 1.
- 3. Il existe des entiers u et v tels que au + bv = d. Si n divise a et b, alors n divise au et bv, par suite n divise d. Réciproquement si n divise d, alors n divise d et d divise a, par conséquent n divise a. De même n divise b.
- 4. Nous avons (ka)u + (kb)v = kd donc kd appartient à  $ka\mathbb{Z} + kb\mathbb{Z} = \operatorname{pgcd}(ka, kb)\mathbb{Z}$ . Ainsi kd est multiple de  $\operatorname{pgcd}(ka, kb)$ . De plus, puisque d divise a et b, kd divise ka et kb, il en résulte que kd divise  $\operatorname{pgcd}(ka, kb)$ .

#### 5. D'après 4., nous avons

$$d \operatorname{pgcd}(a', b') = \operatorname{pgcd}(da', db') = \operatorname{pgcd}(a, b) = d$$

d'où  $\operatorname{pgcd}(a', b') = 1$ .

## Théorème 1.16: (Théorème de Gauss)

Soient a, b et c des entiers non nuls. Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Démonstration. Supposons que a et b soient premiers entre eux; nous avons alors une relation de Bézout : au + bv = 1. Il s'en suit que acu + bcv = c. Si a divise bc, alors a divise (bc)v et a(cu) donc a divise c.

#### Corollaire 1.17

Soit p un nombre premier. Soient b et c deux entiers. Si p divise bc, alors p divise b ou p divise c.

Démonstration. Supposons que p divise bc. Si p ne divise pas b, alors puisque p est un nombre premier, il est premier avec b. Le théorème de Gauss (Théorème 1.16) assure alors que p divise c.

Remarque 3. D'après le Corollaire 1.17 si un nombre premier divise un produit de plusieurs entiers, il divise au moins l'un des facteurs.

## Corollaire 1.18

Soient n, a et b des entiers non nuls. Si n est premier avec a et avec b, alors n est premier avec ab.

Démonstration. Supposons que n soit premier avec a et b. Soit d un diviseur commun à n et ab. Tout diviseur positif commun à d et a divise n et a donc est égal à 1 (car n et a sont premiers entre eux): les entiers d et a sont donc premiers entre eux. Étant donné que d divise ab le théorème de Gauss assure que d divise ab. Ainsi ab divise ab et ab et ab est donc 1. Il en résulte que ab est ab est ab est donc 1. Il en résulte que ab est ab est ab est donc 1. Il en résulte que ab est ab es

Donnons maintenant une application utile du théorème de Gauss :

#### Proposition 1.19

Soit p un nombre premier. Pour tout entier k tel que  $1 \le k \le p-1$ , le coefficient binomial  $\binom{p}{k}$  est un multiple de p.

Démonstration. Par définition  $\binom{p}{k} = \frac{p!}{k!(p-k)!}$  d'où  $p! = \binom{p}{k}k!(p-k)!$ . Ainsi p divise  $\binom{p}{k}k!(p-k)!$ . Supposons que  $1 \le k \le p-1$ ; alors p ne divise aucun entier compris entre 1 et k. Par suite le Corollaire 1.17 assure que p ne divise pas k!. Remarquons que  $1 \le k \le p-1$  implique  $-(p-1) \le -k \le -1$  et  $p-(p-1) \le p-k \le p-1$  qui se réécrit  $1 \le p-k \le p-1$ . Les inégalités  $1 \le p-k \le p-1$  assurent que p ne divise pas non plus (p-k)!. Toujours d'après le Corollaire 1.17 nous en déduisons que p ne divise pas k!(p-k)!. Il s'en suit que p divise  $\binom{p}{k}$ .

# **1.3.3** Équations du type ax + by = c, $a, b \in \mathbb{Z} \setminus \{0\}$ , $c \in \mathbb{Z}$

Soient  $a, b \in \mathbb{Z}$  des entiers non nuls et soit  $c \in \mathbb{Z}$ .

Les nombres de la forme au + bv,  $u, v \in \mathbb{Z}$ , sont les multiples de pgcd(a, b). Nous en déduisons

#### Lemme 1 20

L'équation ax + by = c a des solutions si et seulement si c est un multiple de pgcd(a, b).

Montrons sur un exemple comment trouver toutes les solutions de l'équation.

Exemple 10. Soit  $c \in \mathbb{Z}$ . Trouver tous les  $(x,y) \in \mathbb{Z} \times \mathbb{Z}$  tels que 931x + 513y = c.

- $\diamond$  Si c n'est pas un multiple de  $19 = \operatorname{pgcd}(931, 513)$ , alors l'équation n'a pas de solution.
- $\diamond$  Supposons que  $c=19c', c'\in\mathbb{Z}$ . L'équation 931x+513y=c équivaut alors à 49x+27y=c'.
  - À partir de

$$49 = 27 \times 1 + 22$$
,  $27 = 22 \times 1 + 5$ ,  $22 = 5 \times 4 + 2$ ,  $5 = 2 \times 2 + 1$ 

nous obtenons

$$1 = 5 - 2 \times 2 = 5 - 2 \times (22 - 5 \times 4) = (-2) \times 22 + 9 \times 5$$

$$\iff 1 = (-2) \times 22 + 9 \times (27 - 22 \times 1) = 9 \times 27 + 22 \times (-11)$$

$$\iff 1 = 9 \times 27 + (49 - 27) \times (-11) = 49 \times (-11) + 27 \times 20$$

- Puisque  $49 \times (-11) + 27 \times 20 = 1$ , nous avons  $49 \times (-11c') + 27 \times (20c') = c'$  c'est-à-dire  $(x_0, y_0) = (-11c', 20c')$  est solution.
- Si (x,y) est une solution de l'équation 49x + 27y = c', alors  $49x + 27y = 49x_0 + 27y_0$ , soit  $49(x x_0) + 27(y y_0) = 0$  c'est-à-dire

$$27(y - y_0) = -49(x - x_0).$$

En particulier 27 divise  $49(x-x_0)$ . Comme 27 et 49 sont premiers en eux, le théorème de Gauss assure que 27 divise  $x-x_0$ . Il existe donc  $k \in \mathbb{Z}$  tel que  $x=x_0+27k$ . Il s'en suit

$$27(y - y_0) = -49(x - x_0) = -49 \times 27k$$

d'où  $y - y_0 = -49k$  et  $y = y_0 - 49k$ . Nous vérifions que ces nombres x et y sont bien solution : :

$$49x + 27y = 49(x_0 + 27k) + 27(y_0 - 49k) = 49x_0 + 49 \times 27k + 27y_0 - 27 \times 49k = 49x_0 + 27y_0 = c'.$$

En conclusion l'ensemble des solutions entières de l'équation 931x + 513y = c est

$$\{(-11c' + 27k, 20c' - 49k) \mid k \in \mathbb{Z}\}.$$

# 1.4 Ppcm

#### Définition 1.21

Soient a et b des entiers non nuls. Le ppcm de a et b, noté ppcm(a,b), est le plus petit entier positif multiple de a et de b.

#### Proposition 1.22

Soient a et b des entiers non nuls. Nous avons

$$pgcd(a, b) ppcm(a, b) = ab.$$

Démonstration. Soit d un pgcd de a et b. Posons  $a' = \frac{a}{d}$  et  $b' = \frac{b}{d}$ . Puisque  $d^2a'b')ab$  il suffit de montrer que m = da'b' est un ppcm de a et b. C'est un multiple commun de a (car m = da'b' = ab') et de b (car m = da'b' = ba'). Montrer que m est le ppcm de a et b rest équivalent à montrer que si n est un multiple commun de a et b, alors n est multiple de m. Puisque pgcd(a,b) = d le théorème de Bezout assure l'existence de deux entiers u et v tels que au + bv = d. On en déduit que aun + bvn = dn. Comme an et bn sont multiples de ab, nd est multiple de ab = md. Ainsi n est multiple de m.

#### Proposition 1.23

Soient a et b des entiers non nuls. Pour qu'un entier n soit multiple de a et de b, il faut et il suffit qu'il soit multiple de  $\operatorname{ppcm}(a,b) = \frac{ab}{\operatorname{pgcd}(a,b)}$ .

En particulier, si a et b sont premiers entre eux, alors tout entier multiple de a et de b est multiple de ab.

Démonstration. Posons  $d = \operatorname{pgcd}(a, b), a' = \frac{a}{d}$  et  $b' = \frac{b}{d}$ .

Si n est multiple de  $\frac{ab}{d} = ab' = a'b$ , alors n est multiple de a et b.

Réciproquement, supposons que n soit un multiple de a et b, autrement dit supposons que n=ka et  $n=\ell b$  avec  $k,\,\ell\in\mathbb{Z}$ . Alors  $kda'=\ell db'$  d'où  $d(ka'-\ell b')=0$ . Il en résulte que  $ka'=\ell b'$  et que a' divise  $\ell b'$ . Puisque a' et b' sont premiers entre eux, le théorème de Gauss assure que a' divise  $\ell$ . Par suite il existe  $u\in\mathbb{Z}$  tel que  $\ell=ua'$ . Il s'en suit que  $n=\ell b=ua'b=u\frac{ab}{d}$ ; par conséquent n est multiple de  $\frac{ab}{d}$ .

Exemple 11. Ainsi nous avons ppcm(931,513) =  $\frac{931 \times 513}{\text{pgcd}(931,513)} = \frac{49 \times 19 \times 27 \times 19}{19} = 49 \times 27 \times 19$ .

#### 1.5 Décomposition en facteurs premiers

Nous avons montré que tout entier au moins égal à 2 est produit de nombres premiers ou est premier. Nous allons voir que cette factorisation est essentiellement unique :

#### Proposition 1.24

Pour tout entier a > 1 il existe une unique suite de nombres premiers  $p_1, p_2, \ldots, p_k$  tels que  $a = p_1 p_2 \ldots p_k$  et  $p_1 \le p_2 \le \ldots \le p_k$ .

Démonstration. L'existence est assurée par la Proposition 1.6, en ordonnant les facteurs. Montrons l'unicité. Supposons que  $q_1, q_2, \ldots, q_\ell$  soient des nombres premiers tels que

$$q_1q_2\dots q_\ell=p_1p_2\dots p_k,$$
  $q_1\leq q_2\leq \dots \leq q_\ell.$ 

Si  $p_1 < q_1$ , alors  $p_1 < q_i$  pour tout i, donc  $p_1$  ne divise aucun  $q_i$ ; la Remarque 3 assure alors que  $p_1$  ne divise pas le produit  $q_1q_2 \dots q_\ell$ : contradiction.

Un raisonnement similaire montre que nous ne pouvons pas avoir  $q_1 < p_1$ .

Par suite  $p_1 = q_1$ .

Si  $a=p_1$ , nous avons fini. Sinon, en divisant a par  $p_1$ , nous obtenons  $q_2q_3\dots q_\ell=p_2p_3\dots p_k$ . Si  $\ell < k$ , alors de proche en proche nous obtenons  $1=p_{\ell+1}p_{\ell+2}\dots p_k$ , ce qui est impossible puisque les nombres  $p_i$  ne sont pas égaux à 1. Si  $k < \ell$ , alors de proche en proche nous obtenons  $q_{k+1}p_{k+2}\dots q_\ell=1$ , ce qui est impossible puisque les nombres  $q_i$  ne sont pas égaux à 1. Finalement  $\ell=k$  et  $p_j=q_j$  pour tout  $1 \le j \le k$ .

En regroupant les termes égaux dans la décomposition, nous constatons que tout entier a>1 s'écrit de manière unique à l'ordre près des facteurs :

$$a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$$

où les  $p_i$  sont des nombres premiers deux à deux distincts et  $n_i \geq 1$ .

Par commodité nous étendons cette écriture en considérant un produit sur tous les nombres premiers, y compris ceux qui ne divisent pas a que nous affectons de l'exposant 0: en effet, par convention si q est un entier non nul, alors  $q^0 = 1$ . Notons  $\mathbb{P}$  l'ensemble des nombres premiers, nous écrivons

$$a = \prod_{p \in \mathbb{P}} p^{\nu_p(a)}, \quad \text{où } \nu_p(a) \in \mathbb{N}.$$

Dans ce produit il n'y a bien sûr qu'un nombre fini de facteurs différents de 1 car il n'y a qu'un nombre fini d'exposants non nuls. L'entier  $\nu_p(a)$  s'appelle l'exposant de p dans la décomposition de a en facteurs premiers.

Exemple 12. Nous avons

$$504 = 2 \times 2 \times 2 \times 3 \times 3 \times 7 = 2^3 \, 3^2 \, 7 = \prod_{p \in \mathbb{P}} p^{\nu_p(504)}.$$

où  $\nu_2(504) = 3$ ,  $\nu_3(504) = 2$ ,  $\nu_7(504) = 1$  et  $\nu_p(504) = 0$  pour tout nombre premier p > 7 et p = 5.

La décomposition d'un produit s'obtient en multipliant les décompositions. Pour tout nombre premier p et tous entiers positifs a et b, nous avons donc

$$\nu_p(ab) = \nu_p(a) + \nu_p(b).$$

#### 1.5.1 Expressions du pgcd et du ppcm

Si des entiers a et b ont pour décomposition  $a = \prod_{p \in \mathbb{P}} p^{\nu_p(a)}$  et  $b = \prod_{b \in \mathbb{P}} p^{\nu_p(b)}$ , alors

$$\operatorname{pgcd}(a,b) = \prod_{p \in \mathbb{P}} p^{\min(\nu_p(a),\nu_p(b))}, \qquad \operatorname{ppcm}(a,b) = \prod_{p \in \mathbb{P}} p^{\max(\nu_p(a),\nu_p(b))}.$$

Exemple 13. Considérons

$$n = 172872 = 2^3 \times 3^2 \times 7^4$$
 et  $m = 525525 = 3^1 \times 5^2 \times 7^2 \times 11^1 \times 13^1$ .

Quitte à admettre des puissances nulles nous pouvons écrire la décompositions sur les mêmes facteurs

$$n = 2^3 \times 3^2 \times 5^0 \times 7^4 \times 11^0 \times 13^0$$
 et  $m = 2^0 \times 3^1 \times 5^2 \times 7^2 \times 11^1 \times 13^1$ .

Par conséquent

$$pgcd(m, n) = 2^{0} \times 3^{1} \times 5^{0} \times 7^{2} \times 11^{0} \times 13^{0} = 147$$

et

$$ppcm(m, n) = 2^3 \times 3^2 \times 5^2 \times 7^4 \times 11^1 \times 13^1 = 618017400.$$

#### 1.5.2 Nombres de diviseurs

Soit  $n=p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$  un entier décomposé en facteurs premiers. Pour qu'un entier positif d divise n il faut et il suffit que la décomposition de d soit de la forme

$$d = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$
 où  $0 \le \alpha_i \le n_i$  pour tout  $i$ .

Il y a  $n_1+1$  valeurs possibles pour  $\alpha_1$ ,  $n_2+1$  pour  $\alpha_2$ , etc, par suite : le nombre de diviseurs positifs de  $n=p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$  est  $(n_1+1)(n_2+1)\dots (n_k+1)$ .

Exemple 14. Le nombre de diviseurs positifs de  $4312 = 2^3 \times 7^2 \times 11$  est (3+1)(2+1)(1+1) = 24.

# 1.5.3 Décomposition de n!

Rappelons que la partie entière d'un nombre réel x est le plus grand entier relatif (positif, négatif ou nul) inférieur ou égal à x.

Notée ici E(x), elle est entièrement définie par :

$$\begin{cases} E(x) \in \mathbb{Z} \\ E(x) \le x < E(x) + 1 \end{cases}$$

Soit n un entier au moins égal à 2 et soit p un nombre premier.

- $\diamond$  Parmi les entiers 1, 2, ..., n ceux qui sont multiples de p s'écrivent kp où k est un entier tel que  $1 \le k \le E\left(\frac{n}{p}\right)$ : il y en a  $E\left(\frac{n}{p}\right)$ .
- $\diamond$  Parmi ces multiples de p, ceux qui sont multiples de  $p^2$  sont les  $kp^2$  où k est un entier tel que  $1 \le k \le E\left(\frac{n}{p^2}\right)$ : il y en a  $E\left(\frac{n}{p^2}\right)$ .

- $\diamond$  Parmi 1, 2, ..., n il y a donc  $E\left(\frac{n}{p}\right) E\left(\frac{n}{p^2}\right)$  entiers multiples de p et pas de  $p^2$ .
- $\diamond$  Plus généralement, pour tout entier  $k \geq 1$ , il y a  $E\left(\frac{n}{p^k}\right) E\left(\frac{n}{p^{k+1}}\right)$  entiers multiples de  $p^k$  et pas de  $p^{k+1}$  parmi 1, 2, ..., n.

Nous en déduisons que si  $p^r \le n < p^{r+1}$ , alors

$$\nu_p(n!) = \left(E\left(\frac{n}{p}\right) - E\left(\frac{n}{p^2}\right)\right) + 2\left(E\left(\frac{n}{p^2}\right) - E\left(\frac{n}{p^3}\right)\right) + \ldots + r\left(E\left(\frac{n}{p^r}\right) - E\left(\frac{n}{p^{r+1}}\right)\right).$$

#### Proposition 1.25

Soit n un entier au moins égal à 2. Pour tout nombre premier p, nous avons

$$\nu_p(n!) = E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + \ldots + E\left(\frac{n}{p^k}\right) + \ldots$$

(où la somme n'a qu'un nombre fini de termes).

Exemple 15. Nous avons 
$$\nu_3(25!) = E\left(\frac{25}{3}\right) + E\left(\frac{25}{9}\right) = 8 + 2 = 10.$$

# 2 Relations d'équivalence et ensemble quotient

Nous sommes souvent amenés à partager les éléments d'un ensemble en différentes classes, c'està-dire à définir une partition de cet ensemble. Il devient alors possible de raisonner et de calculer sur les classes : c'est un procédé algébrique puissant.

# 2.1 Partition et relation d'équivalence

# 2.1.1 Partition d'un ensemble

#### Définitions 2 1

multiples de 2 mais pas de 4.

Soit E un ensemble. Une partition de E est la donnée de parties  $C_i$  de E, non vides, deux à deux disjointes et dont la réunion est E. On dit que les parties  $C_i$ ,  $i \in I$  (I ensemble quelconque non vide appelé ensemble des indices), sont des classes.

On peut évidemment définir des partitions de manière totalement arbitraire, par exemple  $\mathbb{N} = \{1, 2, 3, 4\} \cup \{0\} \cup \{n \in \mathbb{N} \mid n \geq 5\}$ , ou bien réunir les éléments qui partagent une propriété commune : Exemple 16. Pour tout entier naturel n notons  $C_n$  l'ensemble des entiers relatifs qui sont divisibles par  $2^n$  mais pas par  $2^{n+1}$ . On a ainsi  $C_0$  qui est l'ensemble des entiers impairs,  $C_1$  l'ensemble des entiers

Les parties  $(C_n)_{n\in\mathbb{N}}$  et  $\{0\}$  forment une partition de  $\mathbb{Z}$ .

On peut aussi utiliser une fonction intermédiaire :

Exemple 17. Soit  $f: E \to F$  une application surjective entre deux ensembles.

Rappelons que pour tout élément  $b \in F$ , la partie de E définie par

$$f^{-1}(b) = \{ x \in E \,|\, f(x) = b \}$$

s'appelle l'image réciproque de b par f.

- $\diamond$  Puisque f est surjective,  $f^{-1}(b)$  est non vide.
- $\diamond$  Les parties  $C_b = f^{-1}(b)$  sont deux à deux disjointes car s'il existe x appartenant à  $C_b \cap C_{b'}$ , alors b = f(x) = b'.
- $\diamond$  De plus leur réunion est E, car pour tout  $x \in E$  nous avons  $x \in f^{-1}(f(x))$  donc x appartient à  $C_{f(x)}$ . Par suite les parties  $C_b$ ,  $b \in F$ , forment une partition de E.

Exemple 18. Soit  $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$  l'application définie par f(x,y) = 2x+3y. L'application f est surjective car pour tout entier  $k \in \mathbb{Z}$ , nous avons f(-k,k) = -2k + 3k = k. Ainsi par exemple les parties

$$C_0 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 2x + 3y = 0\}$$
 et  $C_5 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 2x + 3y = 5\}$ 

sont des classes de la partition de  $\mathbb{Z} \times \mathbb{Z}$  définie par f (droites parallèles à 2x + 3y = 0 intersectées avec  $\mathbb{Z} \times \mathbb{Z}$ ).

En toute généralité, si E est un ensemble et si  $\mathcal{P} = \{C_i\}_{i \in I}$  est une partition de E, on peut dire de deux éléments de E qu'ils sont « reliés » par la partition  $\mathcal{P}$  s'ils appartiennent au même ensemble  $C_i$ . En particulier on constate alors que tout  $x \in E$  est relié à lui-même, que si  $x \in E$  est relié à  $y \in E$  alors y est relié à x et enfin que si x est relié à y et y à y alors y est relié à y. Une telle relation entre les éléments d'un même ensemble est une relation d'équivalence. Il s'agit d'un moyen qui peut s'avérer extrêmement fin pour obtenir des informations sur un ensemble. Dans le paragraphe qui suit nous introduisons plus précisément cette notion.

## 2.1.2 Relation d'équivalence

#### Définition 2.2

Soit E un ensemble. On a défini une relation  $\mathcal{R}$  sur l'ensemble E si on s'est donné un ensemble  $\Gamma \subset E \times E$  appelé graphe de la relation.

Cette définition revient à dire que pour définir une relation, on se donne l'ensemble des couples (x,y) d'éléments de E qui vérifient la relation, i.e.  $(x,y) \in \Gamma$ . Nous avons ici le même mode de définition que pour une application, qui est un cas particulier de relation. Au lieu de noter  $(x,y) \in \Gamma$  nous noterons  $x\mathcal{R}y$ .

#### Définitions 2.3

Une relation  $\mathcal{R}$  sur un ensemble E est une relation d'équivalence si elle est

- (i) réflexive :  $\forall a \in E, a\mathcal{R}a$ ;
- (ii) symétrique :  $\forall a, b \in E, a\mathcal{R}b \Rightarrow b\mathcal{R}a$ ;
- (iii) transitive :  $\forall a, b, c \in E \ (a\mathcal{R}b \text{ et } b\mathcal{R}c) \Rightarrow a\mathcal{R}c;$

Pour tout  $a \in E$ , l'ensemble

$$\overline{a} = \{x \in E \mid x\mathcal{R}a\}$$

s'appelle la classe (d'équivalence) de a.

Exemple 19. Sur tout ensemble E, l'égalité de deux éléments est une relation d'équivalence. Ici  $\Gamma =$  diagonale de  $E \times E$ . En effet définissons sur E la relation  $\mathcal{R}$  par : soient  $x, y \in E$  alors  $x\mathcal{R}y$  si et seulement si x = y. La relation  $\mathcal{R}$  est :

- $\diamond$  réflexive : pour tout x dans E, nous avons x = x, i.e.  $x \mathcal{R} x$ ;
- $\diamond$  symétrique : soient x et y dans E tels que  $x\mathcal{R}y$ , c'est-à-dire x=y; mais x=y si et seulement si y=x, autrement dit  $y\mathcal{R}x$ ;
- $\diamond$  transitive: soient x, y et z dans E tels que  $x\mathcal{R}y$  et  $y\mathcal{R}z$ ; alors d'une part x=y et d'autre part y=z ce qui conduit à x=z, *i.e.*  $x\mathcal{R}z$ .

Pour tout x dans E,  $\overline{x} = \{x\}$ .

Comme on peut s'en douter, ce premier exemple correspond à la relation d'équivalence « triviale ». Les classes d'équivalence y étant réduites à un élément elle n'a concrètement pas une grande utilité. Elle indique cependant que les relations d'équivalence sont en quelque sorte des généralisations de la relation d'égalité.

Exemple 20. Sur l'ensemble des droites (du plan ou de l'espace), la relation « droites parallèles ou confondues » est une relation d'équivalence. Si d est une droite, sa classe d'équivalence  $\overline{d}$  est par définition la direction de d.

Exemple 21. Pour les angles du plan, la relation de congruence modulo  $2\pi$  est une relation d'équivalence. La classe d'équivalence d'un angle  $\vartheta$  par la relation de congruence modulo  $2\pi$  est l'angle lui-même modulo  $2\pi$ :  $C_{\vartheta} = \{\vartheta + 2k\pi \mid k \in \mathbb{Z}\}.$ 

Exemple 22. Dans  $\mathbb{Z}$ , la relation  $x \equiv y \mod (n)$ , que nous noterons aussi  $x \equiv_n y$ , si x - y est divisible par l'entier n est une relation d'équivalence  $\mathbb{R}$ . En effet,  $\mathbb{R}$  est

- $\diamond$  réflexive : pour tout  $x \in \mathbb{Z}$  nous avons x x = 0 est divisible par n, i.e.  $x \in \mathbb{Z}$
- $\diamond$  symétrique : soient x et y dans  $\mathbb{Z}$  tels que  $x\mathcal{R}y$ , c'est-à-dire tels que x-y=nu pour un certain  $u\in\mathbb{Z}$ , alors y-x=n(-u) et  $y\mathcal{R}x$ ;
- $\diamond$  transitive : soient x, y et z dans  $\mathbb{Z}$  tels que  $x\mathcal{R}y$  et  $y\mathcal{R}z$ . Alors d'une part x-y=nu pour un certain  $u\in\mathbb{Z}$  et y-z=nv pour un certain  $v\in\mathbb{Z}$ . Nous en déduisons que

$$x - z = (x - y) + (y - z) = nu + nv = n\underbrace{(u + v)}_{\in \mathbb{Z}}$$

soit  $x\mathcal{R}z$ .

Les classes d'équivalence sont les  $\overline{y} = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, x - y = kn\}$  pour  $y \in \{0, 1, 2, ..., n - 1\}$ , ce qui correspond à l'ensemble des restes possibles de la division euclidienne par n. En effet, par définition

$$\overline{y} = \{x \in \mathbb{Z} \mid x \mathcal{R} y\} = \{x \in \mathbb{Z} \mid x - y \text{ est divisible par } n\} = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} \ x - y = kn\}$$

L'ensemble de ces classes d'équivalence est noté  $\mathbb{Z}/_{n\mathbb{Z}}$ . Nous l'étudierons en détails au §3.

Exemple 23. Notons S l'ensemble des suites de nombres complexes. On dit que  $(x_n) \in S$  est équivalente à  $(y_n) \in S$  s'il existe  $(r_n) \in S$  qui converge vers 1, et  $N \in \mathbb{N}$  tels que pour tout entier  $n \geq N$  on ait  $x_n = r_n y_n$ . Il s'agit d'une relation d'équivalence. En effet, elle est

- $\diamond$  réflexive : avec  $r_n = 1$  pour tout n on a  $x_n = r_n x_n$ .
- $\diamond$  symétrique : soient  $N \in \mathbb{N}$  et  $(r_n)$  convergeant vers 1 tels que pour tout  $n \geq N$  on a  $x_n = r_n y_n$ . Puisque  $(r_n)$  converge vers 1, la suite  $\left(\frac{1}{r_n}\right) = (q_n)$  est bien définie à partir d'un certain rang  $N_1$  et elle converge vers 1. Pour  $n \geq \max(N, N_1)$  on a :  $y_n = q_n x_n$ , ce qui nous indique que  $(y_n)$  est équivalente à  $(x_n)$ .
- $\diamond$  transitive : soient  $(x_n)$  une suite équivalente à  $(y_n)$  elle-même équivalente à  $(z_n)$ . Il existe  $(N_1, N_2) \in \mathbb{N} \times \mathbb{N}$  et  $(r_n) \in \mathcal{S}$  et  $(s_n) \in \mathcal{S}$ , toutes deux convergeant vers 1, tels que pour  $n \geq \max(N_1, N_2) := N$  on a  $x_n = r_n y_n$  et  $y_n = s_n z_n$ . On a alors, pour  $n \geq N$ ,  $x_n = r_n s_n z_n$ . La suite  $(r_n s_n)$  converge vers 1 ce qui permet de conclure que  $(x_n)$  est équivalente à  $(z_n)$ .

Exemple 24. Dans  $E = \mathbb{N} \times \mathbb{N}$ ,  $(a, b)\mathcal{R}(a', b') \iff a + b' = a' + b$  est une relation d'équivalence. En effet, la relation  $\mathcal{R}$  est

- $\diamond$  réflexive : pour tout (a,b) dans E, nous avons a+b=a+b, i.e.  $(a,b)\mathcal{R}(a,b)$ ;
- $\diamond$  symétrique : soient (a,b) et (a',b') dans E tels que  $(a,b)\mathcal{R}(a',b')$ , c'est-à-dire tels que a+b'=a'+b. Or a+b'=a'+b se réécrit a'+b=a+b' donc  $(a',b')\mathcal{R}(a,b)$ .
- $\diamond$  transitive : soient (a,b), (a',b') et (a'',b'') dans E tels que  $(a,b)\mathcal{R}(a',b')$  et  $(a',b')\mathcal{R}(a'',b'')$ . Alors d'une part a+b'=b+a' et d'autre part a'+b''=a''+b'; nous en déduisons que

$$a + b'' = \underbrace{a + b'}_{b + a'} - b' + b'' = b + a' - b' + b'' = b - b' + \underbrace{a' + b''}_{a'' + b'} = b - b' + a'' + b' = a'' + b$$

c'est-à-dire que  $(a,b)\mathcal{R}(a'',b'')$ .

La classe (a,b) de (a,b) est par définition le nombre relatif a-b. En effet, par définition

$$\overline{(a,b)} = \{(a',b') \in E \mid (a',b')\mathcal{R}(a,b)\} = \{(a',b') \in E \mid a'+b=a+b'\} 
= \{(a',b') \in E \mid a'-b'=a-b\}$$

Lorsque l'on construit les ensembles de nombres, cette manière de « symétriser » l'addition de  $\mathbb{N}$  permet, partant de  $\mathbb{N}$ , de construire l'ensemble  $\mathbb{Z}$ . On a en effet très envie d'identifier la classe de (a,b) avec l'entier relatif a-b. On fait en réalité le contraire en définissant (a-b) comme la classe de (a,b). Il faut alors définir une addition naturelle sur l'ensemble des classes d'équivalence, ce que l'on détaillera plus tard.

Exemple 25. Dans  $E = \mathbb{Z} \times \mathbb{Z}^*$ ,  $(p,q)\mathcal{R}(p',q') \iff pq' = p'q$  est une relation d'équivalence. On vérifie en effet qu'elle est :

- $\diamond$  réflexive : pour tout (p,q) dans E, nous avons pq = pq, i.e.  $(p,q)\mathcal{R}(p,q)$ ;
- $\diamond$  symétrique : soient (p,q) et (p',q') dans E tels que  $(p,q)\mathcal{R}(p',q')$ . C'est-à-dire tels que pq'=p'q. Cela se réécrit p'q=pq' donc  $(p',q')\mathcal{R}(p,q)$ .
- $\diamond$  transitive : soient (p,q), (p',q') et (p'',q'') dans E tels que  $(p,q)\mathcal{R}(p',q')$  et  $(p',q')\mathcal{R}(p'',q'')$ . Alors d'une part pq'=p'q et d'autre part p'q''=p''q'; nous en déduisons que

$$\underbrace{pq'}_{p'q}q'' = p'qq'' = q\underbrace{p'q''}_{p''q'} = qp''q' = p''qq'$$

soit pq'' = p''q (car q' appartient à  $\mathbb{Z}^*$ ), *i.e.*  $(p,q)\mathcal{R}(p'',q'')$ . La classe (p,q) de (p,q) est par définition le nombre rationnel  $\frac{p}{q}$ . En effet, par définition

$$\overline{(p,q)} = \{(p',q') \in E \mid (p',q')\mathcal{R}(p,q)\} = \{(p',q') \in E \mid pq' = p'q\} \\
= \{(p',q') \in E \mid \frac{p'}{q'} = \frac{p}{q}\}$$

C'est la multiplication sur  $\mathbb{Z}$  que l'on « symétrise » cette fois et partant de  $\mathbb{Z}$  on construit l'ensemble  $\mathbb{Q}$  en définissant  $\frac{p}{q}$  comme la classe de (p,q). Il convient ensuite de munir l'ensemble des classes d'équivalence d'une addition et d'une multiplication.

Ces deux derniers exemples illustrent la puissance des relations d'équivalence qui permettent de formaliser certaines idées de manière très efficace.

#### Proposition 2.4

Soit  $\mathcal{R}$  une relation d'équivalence sur un ensemble E. Alors

- $\diamond$  pour tout  $a \in E$ ,  $a \in \overline{a}$ ;
- $\diamond$  pour tous  $a, b \in E$  nous avons l'équivalence :  $a\mathcal{R}b \iff \overline{a} = \overline{b}$ ;
- $\diamond$  pour tous  $a, b \in E$ , si  $\overline{a} \neq \overline{b}$ , alors  $\overline{a} \cap \overline{b} = \emptyset$ .

 $D\acute{e}monstration$ . Soient a, b dans E.

- $\diamond$  Puisque d'après (i) nous avons  $a\mathcal{R}a$ , nous obtenons :  $a \in \overline{a}$ .
- $\diamond$  Supposons que  $a\mathcal{R}b$ . Pour tout  $z\in \overline{a}$  nous avons  $z\mathcal{R}a$ ; puisque par hypothèse  $a\mathcal{R}b$ , nous obtenons par transitivité  $z\mathcal{R}b$ . En particulier z appartient à  $\overline{b}$ . Ceci montre que  $\overline{a}\subset \overline{b}$ . Comme  $a\mathcal{R}b$  nous avons par symétrie  $b\mathcal{R}a$ ; de la même façon que précédemment nous obtenons que  $\overline{b}\subset \overline{a}$ . Ainsi  $\overline{a}=\overline{b}$ .

Réciproquement, si  $\bar{a} = \bar{b}$ , alors a qui appartient à  $\bar{a}$  appartient aussi à  $\bar{b}$  et donc  $a\mathcal{R}b$ .

 $\diamond$  Montrons la dernière assertion en raisonnant par contraposée. Supposons que  $\overline{a} \cap \overline{b} \neq \emptyset$ . Soit donc z dans  $\overline{a} \cap \overline{b}$ . Puisque z appartient à  $\overline{a}$  (resp.  $\overline{b}$ ), zRa (resp. zRb). Par symétrie aRz. Par transitivité aRz et zRb conduisent à aRb, soit  $\overline{a} = \overline{b}$ .

Remarquons que E est la réunion des classes d'équivalence car tout élément a de E appartient à  $\overline{a}$ . Nous en déduisons l'énoncé suivant :

19

#### Proposition 2.5

Étant donnée une relation d'équivalence sur E, les classes d'équivalence forment une partition de E.

Réciproquement, et comme nous l'avons déjà indiqué à la fin du paragraphe sur les partitions (§2.1.1), si on se donne une partition  $(C_i)_{i\in I}$  de E, alors la relation définie par  $a\mathcal{R}b \iff (\exists i \in I \text{ tel que } a, b \in C_i)$  est une relation d'équivalence dont les classes sont les  $C_i$ . Ainsi relation d'équivalence et partition sont deux points de vue différents d'un même concept.

# 2.1.3 Relation d'équivalence définie par une application

Soit  $f \colon E \to F$  une application entre deux ensembles. Définissons une relation  $\mathcal{R}_f$  sur E en posant

$$\forall x, y \in E, x\mathcal{R}_f y \iff f(x) = f(y).$$

Cette relation est réflexive, symétrique et transitive. En effet

- $\diamond$  si  $x \in E$ , alors f(x) = f(x), c'est-à-dire  $x \mathcal{R} x$ ;
- $\diamond$  si x, y sont deux éléments de E tels que  $x\mathcal{R}y$ , alors f(x) = f(y) d'où f(y) = f(x) et  $y\mathcal{R}x$ ;
- $\diamond$  si x, y et z sont des éléments de E tels que  $x\mathcal{R}y$  et  $y\mathcal{R}z$ , alors f(x) = f(y) et f(y) = f(z); nous en déduisons que f(x) = f(z), c'est-à-dire  $x\mathcal{R}z$ .

#### Définition 2.6

Soit  $f: E \to F$  une application. La relation d'équivalence  $\mathcal{R}_f$  définie par

$$\forall x, y \in E, x \mathcal{R}_f y \iff f(x) = f(y)$$

s'appelle la relation d'équivalence définie par f.

Pour tout  $a \in E$ , la classe de a est  $\overline{a} = \{x \in E \mid f(x) = f(a)\} = f^{-1}(f(a))$ .

Exemple 26. Soit O un point du plan euclidien E et soit  $f: E \to \mathbb{R}$ , la fonction qui à M associe OM. La relation d'équivalence associée à f est

$$\forall M, M' \in E, M\mathcal{R}_f M' \iff OM = OM'.$$

La classe d'équivalence d'un point  $A \in E$  est formée des points M qui sont à la même distance de O que A:

$$\overline{A} = \{ M \in E \mid M\mathcal{R}_f \} = \{ M \in E \mid OM = OA \}$$

Ainsi:

- $\diamond \underline{\text{si}} A \neq O$ , alors  $\overline{A}$  est le cercle de centre O passant par A,
- $\diamond \overline{O} = \{O\}.$

Exemple 27. Soient E et F deux espaces vectoriels et  $f\colon E\to F$  une application linéaire. Si x et y sont dans E, alors

$$x\mathcal{R}_f y \iff f(x) = f(y) \iff f(x) - f(y) = 0_F \iff f(x - y) = 0_F.$$

Autremenent dit on a  $x\mathcal{R}_f y \iff (x-y) \in \ker f$  (le noyau de l'application linéaire f).

# 2.2 Ensemble quotient

#### Définitions 2.7

Soit  $\mathcal{R}$  une relation d'équivalence sur un ensemble E.

- $\diamond$  L'ensemble des classes d'équivalence s'appelle l'ensemble quotient de E par  $\mathcal{R}$  et se note  $E_{\mathcal{R}}$ :
- $\diamond$  L'application  $p: E \to E/\mathcal{R}$  définie par  $p(x) = \overline{x}$  s'appelle la projection canonique.
- $\diamond$  Étant donnée une classe d'équivalence  $\overline{a}$  tout élément  $x \in \overline{a}$  s'appelle un représentant de cette classe.

# Proposition 2.8

- $\diamond$  L'application p est surjective :  $\forall \alpha \in E/\mathbb{R}$ ,  $\exists a \in E, \alpha = p(a)$ .
- $\diamond$  La relation  $\mathcal{R}$  est la relation d'équivalence définie par p:

$$\forall x, y \in E, p(x) = p(y) \Leftrightarrow x \mathcal{R} y.$$

Démonstration.  $\diamond$  Toute classe  $\alpha \in E/\mathcal{R}$  est la classe d'au moins un élément  $a \in E : \alpha = \overline{a}$ , donc  $\alpha = p(a)$ .

 $\diamond$  Pour tous  $x, y \in E$ , nous avons  $x\mathcal{R}y \iff \overline{x} = \overline{y} \iff p(x) = p(y)$  donc  $\mathcal{R}$  est la relation d'équivalence définie par l'application p.

Toute relation d'équivalence sur E est donc définie par une application : la projection canonique  $E \to E/R$ .

Exemple 28. Considérons la relation sur  $\mathbb{R}^*$  définie par :  $x\mathcal{R}y \iff xy > 0$ .

C'est une relation d'équivalence car

- $\diamond$  elle est réflexive : pour tout  $x \in \mathbb{R}^*$  nous avons  $x^2 > 0$ , i.e. xx > 0, c'est-à-dire  $x\mathcal{R}x$ ;
- $\diamond$  elle est symétrique : soient x, y dans  $\mathbb{R}^*$  tels que  $x\mathcal{R}y$  c'est-à-dire tels que xy > 0, alors yx > 0 soit  $y\mathcal{R}x$ ;
- $\diamond$  elle est transitive : soient x, y et z dans  $\mathbb{R}^*$  tels que  $x\mathcal{R}y$  et  $y\mathcal{R}z$ , *i.e.* tels que xy > 0 et yz > 0; alors  $xy^2z > 0$  et comme  $y^2 > 0$  nous obtenons xz > 0 c'est-à-dire  $x\mathcal{R}z$ .

La relation  $\mathcal{R}$  est la relation d'équivalence définie par l'application  $\operatorname{sgn}: \mathbb{R}^* \to \{1, -1\}$  qui à tout  $x \in \mathbb{R}^*$  associe son signe (avec l'abus de notation 1 pour  $\overline{1}$  et -1 pour  $\overline{-1}$ ).

Il y a deux classes :  $\overline{1} = \mathbb{R}^{*+}$  et  $\overline{-1} = \mathbb{R}^{*-}$ . L'ensemble quotient  $\mathbb{R}^*/\mathcal{R}$  est donc formé de deux éléments :  $\mathbb{R}^*/\mathcal{R} = \{\overline{1}, -\overline{1}\}$ .

# 2.3 Passage au quotient d'une application (\*\*)

Comme nous l'avons vu

- $\diamond$  la notion de relation d'équivalence sur un ensemble X est l'outil qui permet en pratique d'identifier les éléments de X partageant une certaine propriété (les rendant « équivalents » );
- $\diamond$  la donnée d'une telle relation sur X définit une partition naturelle de X en classes d'équivalence ;
- $\diamond$  l'ensemble de ces classes, un sous-ensemble de l'ensemble de toutes les parties de X, est appelé ensemble quotient de X par  $\mathcal{R}$ , et il est noté  $X_{\mathcal{R}}$ .

Sa propriété principale (dite « universelle ») est qu'une application  $f: X \to Y$  constante sur les classes d'équivalence de  $\mathcal{R}$  se factorise canoniquement en une application  $\widetilde{f}: X/\mathcal{R} \to Y$ , appelée passage au quotient de f (voir Théorème 2.9).

Exemple 29. Reprenons la relation de l'Exemple 21 de congruence modulo  $2\pi$ . Étant donné  $\theta \in [0, 2\pi[$  on note  $\overline{\theta} := \{\theta + 2n\pi, n \in \mathbb{Z}\}$  sa classe d'équivalence. On a alors  $E/\mathcal{R} = \bigcup_{\theta \in \mathbb{R}} \overline{\theta}$ . Considérons les fonctions

 $f\colon x\mapsto \cos(x)$  et  $g\colon x\mapsto x+1$ . Il est très tentant de définir « naïvement »  $\overline{f}\colon E/\mathcal{R}\to\mathbb{R}$  et  $\overline{g}\colon E/\mathcal{R}\to\mathbb{R}$  et  $\overline{g}\colon E/\mathcal{R}\to\mathbb{R}$  en posant tout simplement  $\overline{f}(\overline{\theta})=f(\theta)$  et  $\overline{g}(\overline{\theta})=g(\theta)$ . Mais si cela a du sens pour  $\overline{f}$ , cela n'en a aucun pour  $\overline{g}$ . En effet, pour tout  $k\in\mathbb{Z}$  on a  $\overline{\theta}=\overline{\theta+2k\pi}$  alors  $f(\theta)=\cos(\theta)=\cos(\theta+2k\pi)=f(\theta+2k\pi)$ , par contre, si  $k\neq 0$ ,  $g(\theta)=\theta+1\neq \theta+2k\pi+1=g(\theta+2k\pi)$ . La définition « naturelle » a donc un sens pour f, qui est constante sur les classes d'équivalence, mais aucun pour g, qui ne l'est pas.

L'énoncé suivant permet de définir des applications sur un ensemble quotient :

# Théorème 2.9: (Factorisation canonique d'une application)

Soit  $\mathcal{R}$  une relation d'équivalence sur un ensemble E. Soit  $p \colon E \to E/\mathcal{R}$  la projection canonique. Soit  $f \colon E \to F$  une application entre deux ensembles.

Pour qu'il existe une application  $\tilde{f} \colon E/\mathcal{R} \to F$  telle que  $\tilde{f} \circ p = f$  il faut et il suffit que  $\forall x, y \in E, x\mathcal{R}y \Longrightarrow f(x) = f(y)$ .

Dans ce cas

- $\diamond$   $\widetilde{f}$  est unique et pour toute classe  $\alpha \in E/\mathcal{R}$  nous avons  $\widetilde{f}(\alpha) = f(a)$  pour tout représentant a de  $\alpha$ ;
- $\diamond \widetilde{f}$  est injective si et seulement si  $\forall x, y \in E, x \mathcal{R} y \iff f(x) = f(y)$ ;
- $\diamond$  les applications f et f ont la même image.

Si l'application  $\tilde{f}$  existe, nous disons que f passe au quotient modulo  $\mathcal{R}$  et  $\tilde{f}$  s'appelle la factorisation de f par  $E_{\mathcal{R}}$ :



Démonstration.  $\diamond$  Supposons qu'il existe  $\tilde{f}: E/_{\mathcal{R}} \to F$  telle que  $f = \tilde{f} \circ p$ . Si  $x, y \in E$  sont tels que  $x\mathcal{R}y$ , alors p(x) = p(y), donc  $f(x) = \tilde{f}(p(x)) = \tilde{f}(p(y)) = f(y)$ .

Réciproquement supposons que pour tous  $x, y \in E$ , nous ayons la propriété :  $x\mathcal{R}y \Longrightarrow f(x) = f(y)$ . Si  $\alpha \in E/\mathcal{R}$ , alors pour tous représentants a, a' de  $\alpha$  nous avons  $a'\mathcal{R}a$  donc f(a) = f(a'): l'application f prend la même valeur sur tous les représentants de  $\alpha$ . Nous pouvons donc poser

 $\widetilde{f}(\alpha) = f(a)$  où a est un représentant quelconque de  $\alpha$ . Nous définissons ainsi une application  $\widetilde{f} \colon E/\mathbb{R} \to F$  telle que  $\widetilde{f}(p(a)) = f(a)$  quel que soit  $a \in E$ .

 $\diamond$  Supposons que  $\widetilde{f}$  soit injective. Soient  $x, y \in E$  tels que f(x) = f(y). Alors  $\widetilde{f}(p(x)) = \widetilde{f}(p(y))$  donc p(x) = p(y) et par suite  $x\mathcal{R}y$ .

Réciproquement, supposons que pour tous  $x, y \in E$  nous avons  $x\mathcal{R}y \iff f(x) = f(y)$ . Soient x = f(x) at x = f(x) des éléments de  $x \in f(x)$  tels que  $\widetilde{f}(x) = \widetilde{f}(x)$ . Alors  $f(x) = \widetilde{f}(x) = \widetilde{f}(x)$ 

 $\alpha = p(a)$  et  $\beta = p(b)$  des éléments de  $\widetilde{f}(\alpha) = \widetilde{f}(\alpha) = \widetilde{f}(\beta)$ . Alors  $f(a) = \widetilde{f}(\alpha) = \widetilde{f}(\beta) = f(b)$  donc  $a\mathcal{R}b$  et  $\alpha = \beta$ : l'application  $\widetilde{f}$  est donc injective.

 $\diamond$  Puisque  $f = \widetilde{f} \circ p$  nous avons  $f(E) = \widetilde{f}(p(E)) = \widetilde{f}(E/R)$  car p est surjective.

En appliquant le Théorème 2.9 à la relation  $\mathcal{R}_f$  définie par f, nous obtenons l'énoncé très utile suivant.

# Corollaire 2.10: (Factorisation canonique d'une application)

Soit  $f: E \to F$ . Soit  $\mathcal{R}_f$  la relation d'équivalence associée à f. Soit  $p: E \to E/\mathcal{R}_f$  la projection canonique.

- $\diamond$  Il existe une unique application  $\widetilde{f} \colon E/\mathcal{R}_f \to F$  telle que  $\widetilde{f} \circ p = f$ .
- $\diamond$  L'application  $\widetilde{f}$  est injective.
- $\diamond$  L'application  $\widetilde{f}$  est bijective si et seulement si l'application f est surjective.

Démonstration. Dans le Théorème 2.9, prenons  $\mathcal{R}_f$  comme relation d'équivalence sur E. Pour tous x,  $y \in E$  nous avons alors les deux implications

$$x\mathcal{R}_f y \Longrightarrow f(x) = f(y)$$
  $f(x) = f(y) \Longrightarrow x\mathcal{R}_f y$ 

donc f passe au quotient modulo  $\mathcal{R}_f$  et l'application  $\widetilde{f}$  est injective. Par suite l'application  $\widetilde{f}$  est bijective si et seulement si elle est surjective, c'est-à-dire si et seulement si f est surjective car f et  $\widetilde{f}$  ont même image.

Exemple 30. Reprenons un exemple introduit précédemment. Soit O un point du plan euclidien E et soit  $f \colon E \to \mathbb{R}$ , la fonction qui à M associe la distance OM entre O et M. La relation d'équivalence associée à f est

$$\forall M, M' \in E, M\mathcal{R}_f M' \iff OM = OM'.$$

L'ensemble quotient  $E_{\mathcal{R}_f}$  est l'ensemble des cercles de centre O. L'application  $\widetilde{f} \colon E_{\mathcal{R}_f} \to \mathbb{R}$  est définie comme suit : pour tout cercle  $C \in E_{\mathcal{R}_f}$   $\widetilde{f}(C) = OM$  où M est un point quelconque de C. Autrement dit, pour tout cercle C de centre O,  $\widetilde{f}(C)$  est le rayon de C. Cette application est bien injective.

Pour qu'une application  $g: E \to \mathbb{R}$  passe au quotient il faut et il suffit que pour tous  $M, M' \in E$  nous ayons la propriété suivante :  $OM = OM' \Rightarrow g(M) = g(M')$  : cette propriété signifie que pour tout  $M \in E, g(M)$  ne dépend que de la distance OM.

Exemple 31. Dans l'ensemble  $E = \mathbb{Z} \times \mathbb{N}^*$  définissons la relation

$$\forall (x,y), (x',y') \in E, (x,y)\mathcal{R}(x',y') \iff xy' - x'y = 0.$$

C'est une relation d'équivalence (à vérifier en exercice <sup>1</sup>).

Soit  $f : E \to \mathbb{Q}$  l'application définie par  $f(x,y) = \frac{x}{y}$ . Pour tous (x,y), (x',y') dans E nous avons

$$(x,y)\mathcal{R}(x',y') \Longleftrightarrow xy' = x'y \Longleftrightarrow \frac{x}{y} = \frac{x'}{y'} \Longleftrightarrow f(x,y) = f(x',y').$$

Ainsi  $\mathcal{R}$  est la relation définie par f.

En appelant  $p: E \to E/\mathcal{R}$  la projection canonique, il existe donc une application injective  $\widetilde{f}: E \to E/\mathcal{R} \to \mathbb{Q}$  telle que  $\widetilde{f} \circ p = f$ . L'application f est surjective car tout nombre rationnel s'écrit  $\frac{a}{b}$  avec  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}^*$  et  $f(a, b) = \frac{a}{b}$ . Par conséquent l'application  $\widetilde{f}$  est bijective.

L'ensemble quotient  $E_{\mathcal{R}}$  est une construction de  $\mathbb{Q}$  à partir des ensembles  $\mathbb{N}$  et  $\mathbb{Z}$ .

# 3 Congruences et $\mathbb{Z}_{n\mathbb{Z}}$

Dans ce paragraphe nous montrons comment calculer modulo un entier donné. Le théorème de Fermat constitue un résultat particulièrement utile. Nous voyons aussi comment résoudre des systèmes de congruences.

# 3.1 Congruences

#### 3.1.1 Relation de congruence

#### Définition 3.1

Soient a et b des entiers relatifs. On dit que a est congru à b modulo n si a-b est multiple de n. Cette relation se note  $a \equiv b \mod n$ .

Exemples 32.  $\Rightarrow$  141  $\equiv$  9 mod 11 car 141 - 9 = 132 est multiple de 11 (en effet 11  $\times$  12 = 132).

- $\diamond$  Nous avons l'équivalence :  $(a \equiv 0 \mod n) \iff n \mid a$ .
- $\diamond$  Si  $a \equiv b \mod n$ , alors pour tout diviseur positif d de n, nous avons  $a \equiv b \mod d$  (en effet si n divise a b et d divise n alors d divise a b).

#### Proposition 3.2

Soient  $a, b \in \mathbb{Z}$ .

- $\diamond$  Si r est le reste de la division euclidienne de a par n, alors  $a \equiv r \mod n$ .
- $\diamond$  a est congru à b modulo n si et seulement si a et b ont même reste dans la division euclidienne par n.

<sup>1.</sup> On peut ensuite relire l'Exemple 25...

Démonstration. Soient q le quotient et r le reste de la division de a par n. Nous avons a = nq + r; par suite a - r = nq est multiple de b et  $a \equiv r \mod n$ .

Soit r' le reste de la division de b par n. Nous avons b = nq' + r' et

$$a - b = n(q - q') + (r - r').$$

Si r = r', alors a - b = n(q - q') est multiple de b. Réciproquement, supposons que a - b soit un multiple de n. Alors r - r' est multiple de n. Mais r et r' sont compris entre 0 et n - 1 d'où les inégalités -n < r - r' < n. L'unique multiple de n strictement compris entre -n et n est 0, par suite r - r' = 0, c'est-à-dire r = r'.

Soit  $\rho \colon \mathbb{Z} \to \{0, 1, \dots, n-1\}$  l'application qui à tout entier  $x \in \mathbb{Z}$  associe son reste dans la division euclidienne par n. D'après la Proposition 3.2 nous avons pour tous  $x, y \in \mathbb{Z}$  l'équivalence

$$x \equiv y \mod n \iff \rho(x) = \rho(y).$$

Ainsi, la relation de congruence modulo n est la relation d'équivalence sur  $\mathbb{Z}$  définie par l'application  $\rho$ .

#### Corollaire 3.3

La relation  $x \equiv y \mod n$  est une relation d'équivalence sur  $\mathbb{Z}$ .

- $\diamond$  Si  $a \in \mathbb{Z}$ , alors la classe de a est  $\overline{a} = \{a + nk \mid k \in \mathbb{Z}\}.$
- $\diamond$  Les classes d'équivalence sont  $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ ; il y en a n.

Démonstration. Soit  $a \in \mathbb{Z}$ . Pour tout  $x \in \mathbb{Z}$  nous avons par définition :  $x \equiv a \mod n$  si et seulement s'il existe  $k \in \mathbb{Z}$  tel que x - a = nk. Par suite la classe de a est  $\{a + nk \mid k \in \mathbb{Z}\}$ . Si r est le reste de la division de a par n, nous avons  $a \equiv r \mod n$  d'où  $\overline{a} = \overline{r}$ . Les différents restes possibles dans la division par n sont  $0, 1, \ldots, n-1$ ; il en résulte que les classes d'équivalence sont  $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ . Des entiers entre 0 et n-1 ne peuvent être congrus modulo n que s'ils sont égaux ; par conséquent, les classes  $\overline{0}, \overline{1}, \ldots, \overline{n-1}$  sont deux à deux disjointes.

Exemples 33.  $\diamond$  Il y a deux classes de congruence modulo 2 : la classe  $\overline{0} = 2\mathbb{Z}$  qui est formée des entiers pairs, et la classe  $\overline{1} = \{2k+1 \mid k \in \mathbb{Z}\}$  qui est formée des entiers impairs.

♦ Les trois classes de congruence modulo 3 sont

$$\overline{0} = 3\mathbb{Z}, \qquad \overline{1} = \{3k+1 \mid k \in \mathbb{Z}\}, \qquad \overline{2} = \{3k+2 \mid k \in \mathbb{Z}\}.$$

#### 3.1.2 Règles de calcul

#### Proposition 3.4

Soit n un entier au moins égal à 1. Pour tous entiers relatifs a, b, a', b' si  $a \equiv b \mod n$  et  $a' \equiv b' \mod n$ , alors

$$a + a' \equiv b + b' \mod n$$
 et  $aa' = bb' \mod n$ .

Par suite, pour tout  $k \in \mathbb{N}$ , nous avons  $a^k \equiv b^k \mod n$ .

Démonstration. Nous avons

$$(a+a') - (b+b') = (a-b) + (a'-b')$$
(3.1)

et

$$aa' - bb' = (a - b)a' + b(a' - b')$$
(3.2)

Suppsons que  $a \equiv b \mod n$  et  $a' \equiv b' \mod n$ . Alors a - b et a' - b' sont multiples de n. Il en résulte que la somme (a - b) + (a' - b') est multiple de n; d'après (3.1) nous avons  $(a + a') \equiv (b + b') \mod n$ .

De même (a-b)a' et b(a'-b') sont multiples de n; ainsi par (3.2) nous obtenons  $aa'\equiv bb'$  mod n.

Exemple 34. Calculons  $5^k + 1 \mod 6$ .

Puisque  $5 \equiv -1 \mod 6$ , nous avons  $5^k \equiv (-1)^k \mod 6$ .

- $\diamond$  Si k est pair, alors  $(-1)^k = 1$  donc  $5^k + 1 \equiv 2 \mod 6$ .
- $\diamond$  Si k est impair, alors  $(-1)^k = -1$  donc  $5^k + 1 \equiv 0 \mod 6$ .

Ainsi, pour tout entier k positif et impair,  $5^k + 1$  est multiple de 6.

#### Proposition 3.5

Soit p un nombre premier.

Pour tout entier k tel que 0 < k < p, nous avons  $\binom{p}{k} \equiv 0 \mod p$ .

#### Théorème 3.6: (Théorème de Fermat)

Soit p un nombre premier. Pour tout entier  $a \in \mathbb{Z}$ , nous avons  $a^p \equiv a \mod p$ .

Démonstration. Commençons par le cas  $a \ge 0$  et raisonnons par récurrence.

Si a = 0, alors la formule est vraie.

Supposons que a soit un entier positif tel que  $a^p \equiv a \mod p$ . La formule du binôme assure que

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \dots + \binom{p}{k}a^{p-k} + \dots + \binom{p}{p-1}a + 1.$$

La Proposition 3.5 assure que les coefficients  $\binom{p}{1}$ ,  $\binom{p}{2}$ , ...,  $\binom{p}{p-1}$  sont tous congrus à 0 modulo p; par suite

$$(a+1)^p \equiv a^p + 1 \bmod p.$$

En utilisant l'hypothèse de récurrence, nous en déduisons que  $(a+1)^p \equiv a+1 \mod p$ . La formule est donc vraie quel que soit l'entier a > 0.

Supposons que a soit un entier négatif tel que  $a^p \equiv a \mod p$ . D'après ce qui précède nous avons

$$(-1)^p a^p = (-a)^p \equiv -a \mod p.$$

Si p > 2, alors p est impair donc  $(-1)^p = -1$  et par conséquent  $a^p \equiv a \mod p$ . Si p = 2, alors  $(-1)^2 a^2 \equiv a^2 \mod 2$  et  $-1 \equiv 1 \mod 2$ . Il en résulte que  $-a \equiv a \mod 2$ , d'où  $a^2 \equiv a \mod 2$ .

# Corollaire 3.7

Soit p un nombre premier. Pour tout entier  $a \in \mathbb{Z}$  non multiple de p, nous avons  $a^{p-1} \equiv 1 \mod p$ .

Démonstration. Le Théorème de Fermat (Théorème 3.6) assure que  $a^p \equiv a \mod p$ , autrement dit p divise  $a^p - a = a(a^{p-1} - 1)$ . Si p ne divise pas a, alors d'après le théorème de Gauss (Théorème 1.16) p divise  $a^{p-1} - 1$  d'où  $a^{p-1} \equiv 1 \mod p$ .

Exemple 35. Calculons  $666^{999} \mod 13$ .

Il s'agit de trouver l'entier  $r \in \{0, 1, \dots, 12\}$  tel que  $666^{999} \equiv r \mod 13$ .

Nous avons :  $666 = 13 \times 51 + 3$ ; par suite  $666 \equiv 3 \mod 13$ .

Nous en déduisons que  $666^{999} \equiv 3^{999} \mod 13$ .

Le Corollaire 3.7 assure que  $3^{12} \equiv 1 \mod 13$ . Effectuons la division euclidienne de 999 par 12 :  $999 = 12 \times 83 + 3$ . Il vient

$$3^{999} = 3^{12 \times 83 + 3} = 3^{12 \times 83} \times 3^3 = (3^{12})^{83} \times 3^3 \equiv 1^{83} \times 3^3 \equiv 27 \equiv 1 \mod 13.$$

Il en résulte que  $666^{999} \equiv 1 \mod 13$ .

# 3.1.3 Résolution d'équations

**Équation**  $ax \equiv b \mod n$ 

Soit n un entier au moins égal à 2.

#### Proposition 3.8

Pour tout entier  $a \in \mathbb{Z}$  premier à n, il existe un entier  $a' \in \mathbb{Z}$  tel que  $aa' \equiv 1 \mod n$ .

Démonstration. Soit a un entier premier à n. Le théorème de Bézout assure l'existence de deux entiers a',  $n' \in \mathbb{Z}$  tels que aa' + nn' = 1. L'entier aa' - 1 est multiple de n, il s'en suit que  $aa' \equiv 1 \mod n$ .  $\square$ 

Remarque 4. Pour trouver a', il suffit de chercher une relation de Bézout entre a et n.

**Résolution de l'équation.** Soit a un entier premier à n. Pour résoudre l'équation  $ax \equiv b \mod n$ , nous multiplions par a' ce qui donne  $x \equiv a'b \mod n$ . Nous avons bien trouvé les solutions car  $a(a'b) = (aa')b \equiv b \mod n$ .

Exemple 36. Trouvons les entiers x tels que 7x + 11 soit multiple de 36. Un entier x est solution si et seulement si  $7x \equiv -11 \mod 36$ . Nous avons la relation de Bézout  $1 \times 36 - 7 \times 5 = 1$  et la congruence  $(-5) \times 7 \equiv 1 \mod 36$ . Les solutions sont les entiers x tels que  $x \equiv (-5) \times (-11) = 55 \mod 36$ , c'est-à-dire  $x \equiv 19 \mod 36$ .

Système d'équations  $(x \equiv a \mod n, x \equiv b \mod p)$ 

Soient n et p des entiers premiers entre eux.

Nous cherchons les entiers  $x \in \mathbb{Z}$  qui sont congrus à a modulo p et à b modulo p.

♦ Calcul d'une solution.

Nous écrivons une relation de Bézout entre n et p:

$$nu + pv = 1$$
 avec  $u, v \in \mathbb{Z}$ .

Posons  $\alpha = pv$  et  $\beta = nu$ . Nous avons alors

$$\alpha \equiv \left\{ \begin{array}{l} 1 \bmod n \\ 0 \bmod p \end{array} \right. \qquad \beta \equiv \left\{ \begin{array}{l} 0 \bmod n \\ 1 \bmod p \end{array} \right.$$

Nous en déduisons que

$$\alpha a \equiv \left\{ \begin{array}{l} a \mod n \\ 0 \mod p \end{array} \right. \qquad \beta b \equiv \left\{ \begin{array}{l} 0 \mod n \\ b \mod p \end{array} \right.$$

Ainsi l'entier  $x_0 = \alpha a + \beta p$  est une solution du système d'équations.

♦ Calcul de toutes les solutions.

Pour tout entier  $x \in \mathbb{Z}$  nous avons les équivalences

$$\begin{cases} x \equiv a \mod n \\ x \equiv b \mod p \end{cases} \iff x \equiv x_0 \mod n \text{ et } x \equiv x_0 \mod p \\ \iff x - x_0 \text{ est multiple de } n \text{ et de } p \\ \iff x - x_0 \text{ est multiple de } np \end{cases}$$

car n et p étant premiers entre eux, nous avons  $\operatorname{ppcm}(n,p) = np$ . Les solutions sont donc les entiers x de la forme  $x_0 + knp$  avec  $k \in \mathbb{Z}$ .

Exemple 37. Trouver les entiers x tels que

$$\begin{cases} x \equiv 3 \mod 8 \\ x \equiv 2 \mod 21 \end{cases}$$

♦ Calcul d'une solution.

Nous avons la relation de Bézout  $8 \times 8 - 21 \times 3 = 1$  et les congruences

$$-63 \equiv \begin{cases} 1 \mod 8 \\ 0 \mod 21 \end{cases}$$
 et 
$$64 \equiv \begin{cases} 0 \mod 8 \\ 1 \mod 21 \end{cases}$$

L'entier  $x_0 = -63 \times 3 + 64 \times 2 = -61$  est donc solution.

Calcul de toutes les solutions.

Pour qu'un entier x soit solution il faut et il suffit que x soit congru à -61 modulo 8 et modulo 21, c'est-à-dire que x+61 soit multiple de 8 et de 21. Puisque  $ppcm(8,21)=8\times 21=168$ , les solutions sont les entiers de la forme -61+168k avec  $k\in\mathbb{Z}$ .

# 3.2 $\mathbb{Z}_{n\mathbb{Z}}$

Nous nous proposons dans ce paragraphe de remplacer l'écriture  $a \equiv b \mod n$  par l'écriture équivalente  $\overline{a} = \overline{b}$  dans  $\mathbb{Z}_{n\mathbb{Z}}$ .

Soit  $n \geq 1$  un entier. Nous appelons  $\mathbb{Z}/_{n\mathbb{Z}}$  l'ensemble quotient de  $\mathbb{Z}$  par la relation d'équivalence « est congru à » (modulo n).

Exemple 38. Pour n=2, soit a un entier. Si a est pair, alors  $\overline{a}$  pour la relation de congruence modulo 2 est l'ensemble P de tous les nombres pairs. Si a est impair, alors  $\overline{a}$  est l'ensemble I de tous les nombres impairs. Finalement  $\mathbb{Z}_{2\mathbb{Z}} = \{I, P\}$ .

Pour tout  $n \ge 1$ ,  $\mathbb{Z}_{n\mathbb{Z}}$  possède n éléments.

Démonstration. Cet énoncé découle du Corollaire 3.3.

La Proposition 3.4 conduit à :

Soient  $\overline{a}$  et  $\overline{b}$  deux éléments de  $\overline{\mathbb{Z}}_{n\mathbb{Z}}$ . Nous définissons  $\diamond$  la somme de  $\overline{a}$  et  $\overline{b}$  par  $\overline{a} + \overline{b} = \overline{a+b}$ 

- $\diamond$  et leur produit  $\overline{a}\,\overline{b} = \overline{ab}$ .