

ARITHMÉTIQUE DANS  
L'ANNEAU  $(\mathbb{Z}, +, \cdot)$ 

## 15.1 DIVISIBILITÉ

§1 La relation « divise » dans  $\mathbb{Z}$ 

## Définition 1

Soit  $(a, b) \in \mathbb{Z}^2$ . On dit que  $a$  **divise**  $b$ , et l'on note  $a \mid b$  lorsqu'il existe  $q \in \mathbb{Z}$  tel que  $b = aq$ .  
Dans ce cas, on dit aussi que  $a$  est un **diviseur** de  $b$  ou que  $b$  est un **multiple** de  $a$ .

## Notation

- On note par  $a\mathbb{Z} = \{ aq \mid q \in \mathbb{Z} \}$  l'ensemble des multiples de  $a$ .
- On note  $D(b) = \{ a \in \mathbb{N} \mid a \mid b \}$  l'ensemble des diviseurs positifs de  $b$ .

## Exemples 2

1.  $5 \mid 210, 3 \mid 18$ .
2.  $D(6) = \{ 1, 2, 3, 6 \}$ .
3.  $4\mathbb{Z} = \{ \dots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \dots \}$ .
4. 0 est divisible par n'importe quel entier et le seul entier divisible par 0 est 0.  

$$\forall a \in \mathbb{Z}, a \mid 0 \text{ et } (0 \mid a \iff a = 0).$$
5. Le seul diviseurs de 1 est 1, mais 1 divise tout entier relatif.  

$$\forall b \in \mathbb{Z}, 1 \mid b.$$

**Proposition 3****Lien avec la relation  $\leq$** 

La divisibilité est liée à l'ordre naturel sur  $\mathbb{Z}$  par

$$\forall b \in \mathbb{Z}, \forall a \in \mathbb{Z}, a \mid b \implies (b = 0 \text{ ou } |a| \leq |b|).$$

La réciproque est fausse.

*Démonstration.* Pour tout  $k \geq 1$ , on a  $k|a| \geq |a|$ . ■

**Proposition 4****Propriétés de la relation  $\mid$  sur  $\mathbb{Z}$** 

La relation  $\mid$  sur  $\mathbb{Z}$  est

1. réflexive :  $\forall a \in \mathbb{Z}, a \mid a$  ;
2. transitive :  $\forall (a, b, c) \in \mathbb{Z}^3, (a \mid b \text{ et } b \mid c) \implies a \mid c$  ;

*Démonstration.* 1. Soit  $a \in \mathbb{Z}$ . On a  $a = a \times 1$  et  $1 \in \mathbb{Z}$ , donc  $a \mid a$ .

2. Soient  $a, b, c \in \mathbb{Z}$  tels que  $a \mid b$  et  $b \mid c$ . Il existe donc  $p, q \in \mathbb{Z}$  tels que  $b = qa$  et  $c = pb$ , d'où

$$c = (qp)a \text{ et } qp \in \mathbb{Z},$$

c'est-à-dire,  $a \mid c$ . ■

**Corollaire 5**

Soit  $(a, b) \in \mathbb{Z}^2$ .

$$a \mid b \iff b \in a\mathbb{Z} \iff b\mathbb{Z} \subset a\mathbb{Z}.$$

**Définition 6**

Soit  $(a, b) \in \mathbb{Z}^2$ . On dit que les entiers  $a$  et  $b$  sont **associés** si  $(a \mid b \text{ et } b \mid a)$ .

**Proposition 7****Caractérisation des couples d'entiers associés**

Soit  $(a, b) \in \mathbb{Z}^2$ . Les assertions suivantes sont équivalentes

1.  $a$  et  $b$  sont associés.
2.  $a\mathbb{Z} = b\mathbb{Z}$ .
3.  $a = b$  ou  $a = -b$ .

## §2 Compatibilité avec les opérations algébriques

### Proposition 8

#### Compatibilité avec les opérations algébriques

Soit  $(a, b, c, d) \in \mathbb{Z}^4$ .

1. *Combinaison linéaire à coefficients entiers* : si  $a \mid b$  et  $a \mid c$ , alors

$$\forall (u, v) \in \mathbb{Z}^2 \quad a \mid ub + vc.$$

En particulier, si  $a \mid b$  et  $a \mid c$ , alors  $a \mid b + c$  et  $a \mid b - c$ .

2. *Produit* : Si  $a \mid b$  et  $c \mid d$ , alors  $ac \mid bd$ .

En particulier, si  $a \mid b$  alors pour tout  $k \in \mathbb{N}$ ,  $a^k \mid b^k$ .

3. *Multiplication/division par un entier* : si  $c \neq 0$ , alors  $a \mid b \iff ac \mid bc$ .

*Démonstration.* 1. Supposons  $a \mid b$  et  $a \mid c$ , alors il existe  $p, q \in \mathbb{Z}$  tels que  $b = pa$  et  $c = qa$ . Pour tout  $u, v \in \mathbb{Z}$ , on a

$$ub + vc = upa + vqa = (up + vq)a \text{ et } up + vq \in \mathbb{Z},$$

c'est-à-dire,  $a \mid ub + vc$ .

2. Supposons  $a \mid b$  et  $c \mid d$ , alors il existe  $p, q \in \mathbb{Z}$  tels que  $b = pa$  et  $d = cq$ . Alors

$$bd = (pa)(cq) = (pq)(ac) \text{ et } pq \in \mathbb{Z},$$

c'est-à-dire,  $ac \mid bd$ .

3. ( $\implies$ ) On a toujours  $c \mid c$ , donc si  $a \mid b$ , on a  $ac \mid bc$ .

( $\impliedby$ ) Si  $ac \mid bc$  et  $c \neq 0$ , alors il existe  $q \in \mathbb{Z}$  tel que  $bc = acq$ , en divisant cette égalité par  $c \neq 0$ , on obtient

$$b = aq \text{ et } q \in \mathbb{Z},$$

c'est-à-dire,  $a \mid b$ .

■

## 15.2 DIVISION EUCLIDIENNE

### §1 Division euclidienne

#### Définition 9

##### Division euclidienne dans $\mathbb{Z}$

Soient  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}^*$ . Alors il existe un unique couple d'entiers  $(q, r) \in \mathbb{Z} \times \mathbb{N}$  vérifiant

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

- $q$  est le **quotient** de la division euclidienne de  $a$  par  $b$ .
- $r$  est le **reste** de la division euclidienne de  $a$  par  $b$  et on le note  $a \bmod b$ .

L'opération qui remplace  $a$  par  $r$  s'appelle la **réduction modulo  $b$** .

*Démonstration.* • Commençons prouver l'unicité d'un couple  $(q, r) \in \mathbb{Z} \times \mathbb{N}$  tel que  $a = bq + r$  et  $0 \leq r < b$ . Supposons l'existence de deux couples  $(q, r)$  et  $(q', r')$  vérifiant ces conditions. Alors  $a = qb + r = q'b + r'$ , d'où  $r - r' = b(q - q')$ ; ainsi  $b$  divise  $|r - r'|$ . Puisque  $0 \leq r < b$  et  $0 \leq r' < b$ , on en déduit  $-b < r - r' < b$ , c'est-à-dire  $0 \leq |r - r'| < b$ . Or le seul multiple de  $b$  dans  $[0, b[$  est 0, on a donc  $r = r'$ . Puisque  $r - r' = b(q - q')$  et  $b \neq 0$ , on a par conséquent  $q = q'$ .

- Soit  $E = \{k \in \mathbb{Z} \mid kb \leq a\}$ . Cet ensemble est une partie non vide et majorée de  $\mathbb{Z}$ . En effet, si  $a \geq 0$ ,  $0 \in E$  et  $a$  majore  $E$  (car  $b \geq 1$ ). Si  $a < 0$ , alors 0 majore  $E$ .

L'ensemble  $E$  admet donc un plus grand élément  $q$ . On a donc  $qb \leq a < (q + 1)b$  (sinon  $q + 1 \in E$ ) et en posant  $r = a - bq$ , on a bien  $0 \leq r < b$ . ■

#### Exemple 10

$$\begin{array}{r|l} 543 & 17 \\ 33 & 31 \\ 16 & \end{array} \quad \text{Ici } a = 543, b = 17, q = 31, r = 16.$$

#### Proposition 11

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

$$b \mid a \iff r = 0.$$

## §2 Sous-groupes de $(\mathbb{Z}, +)$

### Définition 12

Une partie  $A$  de  $\mathbb{Z}$  est appelée **sous-groupe** (additif) de  $\mathbb{Z}$  si elle vérifie les conditions ci-dessous:

1.  $0 \in A$ .

2.  $A$  est **stable pour l'addition**:

$$\forall (x, y) \in A^2, x + y \in A.$$

3.  $A$  est **stable par passage à l'opposé**:

$$\forall x \in A, -x \in A.$$

### Théorème 13

1. Pour tout entier  $a \in \mathbb{Z}$ ,  $a\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$ .

2. Réciproquement, soit  $A$  un sous-groupe de  $\mathbb{Z}$ , il existe un unique entier  $a \geq 0$  tel que

$$A = a\mathbb{Z}.$$

### Proposition 14

Soient  $A$  et  $B$  deux sous-groupes de  $\mathbb{Z}$ , alors l'intersection  $A \cap B$  de ces deux sous-groupes est un sous-groupe de  $\mathbb{Z}$ .

### Proposition 15

Soient  $A$  et  $B$  deux sous-groupes de  $\mathbb{Z}$ , alors la somme de ces deux sous-groupes

$$A + B = \{ x + y \mid x \in A \text{ et } y \in B \}$$

est un sous-groupe de  $\mathbb{Z}$ .

## 15.3 LES NOMBRES PREMIERS

### §1 Définition

### Définition 16

Un **nombre premier** est un entier naturel  $p \geq 2$  dont les seuls diviseurs strictement positifs sont 1 et  $p$ . On note  $\mathbb{P}$  l'ensemble des nombres premiers.

Avec des quantificateurs, cela s'écrit

$$\forall (a, b) \in \mathbb{N}, p = ab \implies a = 1 \text{ ou } b = 1.$$

### Proposition 17

Pour qu'un entier  $p > 1$  soit premier, il faut et il suffit qu'il ne soit pas produit de deux entiers strictement plus grand que 1.

**Théorème 18****(Euclide)**

Tout entier  $n > 1$  est un produit (fini) de nombres premiers. En particulier,  $n$  possède au moins un diviseur premier.

**§2 Crible d'Erathosthène****Proposition 19**

Soit  $n > 1$ . Si  $n$  n'est pas premier, il possède un facteur premier  $p$  tel que  $p^2 \leq n$ .

**Algorithme 20****Crible d'Erathosthène**

Si l'entier  $n$  n'est divisible par aucun nombre premier  $p$  tel que  $p^2 \leq n$ , alors  $n$  est un nombre premier.

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

**§3 Ensemble des nombres premiers****Théorème 21**

L'ensemble  $\mathbb{P}$  des nombres premiers est infini.

De très nombreuses preuves de ce résultat existent. Proposons ici la démonstration d'Euclide, sans doute la plus connue, en raisonnant par l'absurde.

*Démonstration.* Supposons que l'ensemble des nombres premiers  $\mathbb{P}$  soit fini. On peut alors écrire  $\mathbb{P} = \{p_1, \dots, p_k\}$ . On introduit l'entier  $n = p_1 p_2 \dots p_k + 1 \geq 2$ . Cet entier a un diviseur premier  $p$ . Ce nombre premier  $p$  est donc l'un des  $p_i$ . Or  $p$  divise  $n$  et divise  $p_1 p_2 \dots p_k = n - 1$ , donc  $p$  divise  $(n - 1) - n = -1$ , ce qui est absurde. ■

## 15.4 PLUS GRAND COMMUN DIVISEUR, ALGORITHME D'EUCLIDE

### §1 Plus grand commun diviseur de deux entiers

#### Définition 22

Soient  $a$  et  $b$  deux entiers relatifs quelconques. On appelle **plus grand commun diviseur** (ou pgcd) de  $a$  et  $b$  l'unique entier  $d \geq 0$  tel que

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z},$$

on note cet entier  $\text{pgcd}(a, b)$  ou  $a \wedge b$ .

#### Théorème 23

Soient  $a$  et  $b$  deux entiers relatifs quelconques et  $d = \text{pgcd}(a, b)$ .

1. L'entier  $d$  divise  $a$  et  $b$ .
2. Réciproquement, tout diviseur commun à  $a$  et  $b$  divise  $d$ .
3. On a la **relation de Bézout**:

$$\exists (u, v) \in \mathbb{Z}^2, ua + vb = d.$$

4. Si  $a$  et  $b$  sont deux entiers relatifs non nuls, alors

$$\text{pgcd}(a, b) = \max \left\{ n \in \mathbb{N} \mid n \mid a \text{ et } n \mid b \right\}.$$

#### Test 24

Déterminer le pgcd de 105 et 48.

#### Remarque

- On a toujours  $\text{pgcd}(0, 0) = 0$ .
- On a toujours  $\text{pgcd}(a, 0) = |a|$ .
- Si  $a, b \in \mathbb{Z}$ ,  $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$ .
- $a$  divise  $b$  si, et seulement si,  $\text{pgcd}(a, b) = |a|$ .

#### Remarque

<sup>(iii)</sup> La relation divise est une relation d'ordre dans  $\mathbb{N}$  (mais pas dans  $\mathbb{Z}$ ). Pour tous  $a, b \in \mathbb{N}$ , le pgcd de  $a$  et  $b$  est le plus grand (pour la relation divise) des minorants (c'est-à-dire les diviseurs) de  $\{a, b\}$ . Autrement dit,  $\text{pgcd}(a, b)$  est la borne inférieure de  $\{a, b\}$  pour la relation divise dans  $\mathbb{N}$ .

## §2 Entiers premiers entre eux

### Définition 25

Soient  $a, b \in \mathbb{Z}$ . On dit que  $a$  et  $b$  sont **premiers entre eux** lorsque leur seuls diviseurs communs sont  $-1$  et  $1$ :

$$\forall d \in \mathbb{Z}, (d \mid a \text{ et } d \mid b \implies d = \pm 1).$$

### Théorème 26

#### Égalité de Bézout

Soient  $a$  et  $b$  deux entiers. Les assertions suivantes sont équivalentes

1. Les entiers  $a$  et  $b$  sont premiers entre eux.
2.  $\text{pgcd}(a, b) = 1$
3.  $\exists (u, v) \in \mathbb{Z}^2, ua + vb = 1$ .

### Définition 27

Le nombre des entiers  $k$  vérifiant

$$1 \leq k \leq n \quad \text{et} \quad \text{pgcd}(k, n) = 1$$

est noté  $\varphi(n)$ . L'application  $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$  ainsi définie s'appelle **indicateur d'Euler**.

### Définition 28

Soient  $a_1, a_2, \dots, a_r \in \mathbb{Z}$ .

- On dit que  $a_1, \dots, a_r$  sont **premiers entre eux dans leur ensemble** si leurs seuls diviseurs communs sont  $\pm 1$ .
- On dit que  $a_1, \dots, a_r$  sont **premiers entre eux deux à deux** à deux  $a_i$  et  $a_j$  sont premiers entre eux pour tous  $i, j \in \llbracket 1, r \rrbracket$  distincts.

## §3 Lemme de Gauß, lemme d'Euclide

### Théorème 29

#### Lemme de Gauß

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

*Démonstration.* Il existe des entiers  $u, v, w$  tel que  $ua + vb = 1$  et  $bc = aw$ . On peut donc écrire

$$c = uac + vbc = uac + vaw = a(uc + vw).$$

■

### Théorème 30

#### Lemme d'Euclide

Un entier  $p \geq 2$  est un nombre premier si et seulement si il vérifie la condition

$$\forall (a, b) \in \mathbb{Z}^2, p \mid ab \implies (p \mid a \text{ ou } p \mid b);$$

appelée lemme d'Euclide.



*Démonstration.* C'est un cas particulier du lemme de Gauß. Ou bien  $p$  divise  $a$ , ou bien il est premier avec  $a$  et il divise alors  $b$ . ■

*Une démonstration directe, sans utiliser le lemme de Gauß.*

Soit  $p$  premier divisant  $ab$  mais pas  $a$ . Nous devons donc montrer que  $p$  divise  $b$ .

L'ensemble  $A$  des entiers  $n > 0$  tels que  $p$  divise  $an$  contient  $p$ ,  $b$  et  $m = \min A > 0$ , mais pas 1, donc  $m > 1$ .

Pour tout  $n \in A$ , effectuons la division euclidienne  $n = mq + r$ , avec  $0 \leq r < m$ ; alors  $p$  divise  $an - (am)q = ar$ . Comme  $r < m$ , on a  $r \notin A$ , d'où  $r = 0$ , ce qui montre que  $m$  divise  $n$ . En particulier,  $m$  divise  $p$  et  $b$ . Or  $p$  est premier et  $m > 1$ , donc  $p = m$ , qui divise ainsi  $b$ . ■

### Corollaire 31

1. Si  $p$  premier divise  $a_1 a_2 \cdots a_n$ , il divise au moins l'un des facteurs.
2. Si  $p$  premier divise  $a^n$ , ( $n \in \mathbb{N}^*$ ), alors il divise  $a$ .

### Théorème 32

1. Si  $a$  est premier avec  $b$  et  $c$ , alors  $a$  est premier avec  $bc$ .
2. Si  $a$  et  $b$  sont premiers entre eux, et que  $a \mid c$  et  $b \mid c$ , alors  $ab \mid c$ .

*Démonstration.* À faire (exercice!). ■

## §4 Algorithme d'Euclide

### Théorème 33

Soient des entiers  $a$  et  $b$ .

1. Soit  $k$  un entier, alors  $\text{pgcd}(a, b) = \text{pgcd}(a - kb, b)$ .
2. Si  $b > 0$ ,  $\text{pgcd}(a, b) = \text{pgcd}(b, r)$  avec  $r = a \bmod b$ .
3. Soit un entier  $m > 0$ , alors  $\text{pgcd}(ma, mb) = m \times \text{pgcd}(a, b)$ .
4. Soit un entier  $d > 0$ ; si  $d$  divise  $a$  et  $b$ , soient  $a' = da'$  et  $b = db'$ . Alors  $d$  est le  $\text{pgcd}$  de  $a$  et  $b$  si, et seulement si,  $a'$  et  $b'$  sont premiers entre eux.

### Algorithme 34

#### Algorithme d'Euclide

On pose  $r_0 = a$ ,  $r_1 = b$ , puis pour tout  $k$  jusqu'à avoir  $r_N = 0$ ,

$$r_{k+2} = r_k \bmod r_{k+1},$$

c'est-à-dire  $r_{k+2}$  est le reste dans la division euclidienne de  $r_k$  par  $r_{k+1}$ .

Alors  $\text{pgcd}(a, b) = r_{N-1}$ .

### Exemple 35

On a  $\text{pgcd}(105, 48) = 3$ .

En «remontant les calculs», cela permet de trouver des entiers  $u, v \in \mathbb{Z}$  tels que

$$105u + 48v = 3.$$

**Algorithme 36**    **Algorithme d'Euclide étendu**

On peut supposer que  $0 \leq b \leq a$  et on note  $r_0 = a$  et  $r_1 = b$ . Tant que  $r_{k+1} > 0$ , on effectue la division euclidienne de  $r_k$  par  $r_{k+1}$ :

$$r_k = q_{k+2}r_{k+1} + r_{k+2}.$$

La suite ainsi construite est finie, de rang final  $N$  pour lequel  $R_N = 0$ .

On définit alors deux nouvelles suite finies  $(u_k)_{0 \leq k \leq N}$  et  $(v_k)_{0 \leq k \leq N}$  par les relations

$$(u_0, v_0) = (1, 0)$$

$$(u_1, v_1) = (0, 1)$$

$$\forall k \in \llbracket 0, N-2 \rrbracket, (u_{k+2}, v_{k+2}) = (u_k - q_{k+2}u_{k+1}, v_k - q_{k+2}v_{k+1}).$$

On vérifie alors par récurrence que pour tout  $k \in \llbracket 0, N \rrbracket$ ,

$$H(k) : r_k = au_k + bv_k.$$

En effet, on on a

$$r_0 = a = a \times 1 + b \times 0 = au_0 + bv_0$$

$$\text{et } r_1 = b = a \times 0 + b \times 1 = au_1 + bv_1.$$

D'où  $H(0)$  et  $H(1)$ . Soit  $k \in \llbracket 0, N-2 \rrbracket$ . On suppose  $H(k)$  et  $H(k+1)$ , c'est-à-dire

$$r_k = au_k + bv_k \quad \text{et} \quad r_{k+1} = au_{k+1} + bv_{k+1}.$$

Alors

$$\begin{aligned} r_{k+2} &= r_k - q_{k+2}r_{k+1} \\ &= (au_k + bv_k) - q_{k+2}(au_{k+1} + bv_{k+1}) && \because H(k) \text{ et } H(k+1) \\ &= a(u_k - q_{k+2}u_{k+1}) + b(v_k - q_{k+2}v_{k+1}) \\ &= au_{k+2} + bv_{k+2}. \end{aligned}$$

d'où  $H(k)$  et  $H(k+1) \implies H(k+2)$ .

D'après le principe de récurrence, la relation  $H(k)$  est donc vérifiée pour tout  $k \in \llbracket 0, N \rrbracket$ , en particulier

$$\text{pgcd}(a, b) = R_{N-1} = au_{N-1} + bv_{N-1}.$$

## §5 Plus petit commun multiple de deux entiers

**Définition 37**

Soient  $a$  et  $b$  deux entiers relatifs quelconques. On appelle **plus petit commun multiple** (ou ppcm) de  $a$  et  $b$  l'unique entier  $m \geq 0$  tel que

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z},$$

on note cet entier  $\text{ppcm}(a, b)$  ou  $a \vee b$ .

**Théorème 38**

Soient  $a$  et  $b$  deux entiers relatifs quelconques et  $m = \text{ppcm}(a, b)$ .

1. L'entier  $m$  est un multiple de  $a$  et de  $b$ .
2. Réciproquement, tout multiple commun à  $a$  et  $b$  est multiple de  $m$ .
3. Si  $a$  et  $b$  sont deux entiers relatifs non nuls, alors

$$\text{ppcm}(a, b) = \min (a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*).$$

## §6 Généralisation

**Définition 39**

Soient  $a_1, a_2, \dots, a_r \in \mathbb{Z}$ .

- On appelle **plus grand commun diviseur** de  $a_1, \dots, a_r$  l'unique entier naturel  $d$  pour lequel

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_r\mathbb{Z} = d\mathbb{Z}.$$

- On appelle **plus petit commun multiple** de  $a_1, \dots, a_r$  l'unique entier naturel  $m$  pour lequel

$$a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \dots \cap a_r\mathbb{Z} = m\mathbb{Z}.$$

## 15.5 DÉCOMPOSITION EN FACTEURS PREMIERS

### §1 Facteurs premiers d'un entier. Le théorème de décomposition

**Théorème 40**

#### Décomposition en facteurs premiers

Soit  $n \in \mathbb{N}$  tel que  $n \geq 2$ . Alors  $n$  admet une factorisation unique en facteurs premiers, à l'ordre des facteurs près, c'est-à-dire

$$\exists ! m \in \mathbb{N}^*, \exists ! (p_1, \dots, p_m) \in \mathbb{P}^m, p_1 \leq p_2 \leq \dots \leq p_m \text{ et } n = p_1 p_2 \dots p_m.$$

**Exemple 41**

$$90 = 9 \times 10 = 3 \times 3 \times 2 \times 5 = 2 \times 3 \times 3 \times 5 = 2 \times 3^2 \times 5.$$

## §2 Valuation $p$ -adique

### Définition 42

La décomposition de  $n \geq 2$  en facteurs premiers peut également s'écrire sous la forme

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$$

où

- les  $p_i$  sont des nombres premiers deux à deux distincts,
- $\alpha_i \geq 1$ .

Cette écriture est unique, à l'ordre des facteurs près.

- L'entier  $\alpha_i$  est appelé **exposant** du nombre premier  $p_i$  dans la décomposition de  $n$  en facteur premier et noté  $v_{p_i}(n)$ .
- Si  $p$  est un nombre premier distinct de  $p_1, \dots, p_r$ , on pose  $v_p(n) = 0$ .

On dit que  $v_p(n)$  est la **valuation  $p$ -adique** de  $n$ , on a donc

$$v_p(n) = \max \left\{ k \in \mathbb{N} \mid p^k \mid n \right\}.$$

### Proposition 43

Soit  $a, b \in \mathbb{N}^*$ , et  $p \in \mathbb{P}$ . On a

$$v_p(ab) = v_p(a) + v_p(b).$$

### Proposition 44

Soit  $a, b \in \mathbb{N}^*$ , alors  $a \mid b$  si, et seulement si

$$\forall p \in \mathbb{P}, v_p(a) \leq v_p(b).$$

### Proposition 45

Soit  $n$  un entier non nul qui se décompose en produit de facteurs premiers (distincts) de la façon suivante

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$$

Alors, les diviseurs de  $n$  dans  $\mathbb{N}^*$  sont les entiers naturels de la forme

$$d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \dots \cdot p_r^{\gamma_r}, \quad \text{avec } 0 \leq \gamma_i \leq \alpha_i \text{ pour } i = 1 \dots r.$$

### Test 46

Quels sont les diviseurs de 90?

### §3 Applications

**Proposition 47**

Soit  $a$  et  $b$  deux entiers non nuls qui se décomposent en produits de facteurs premiers (distincts) de la façon suivante

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_r^{\beta_r}$$

où les  $\alpha_i$  et  $\beta_i$  sont des entiers éventuellement nuls. Alors

$$\text{pgcd}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \times p_2^{\min(\alpha_2, \beta_2)} \times \dots \times p_r^{\min(\alpha_r, \beta_r)}$$

**Test 48**

Retrouver le pgcd de 105 et 48.

**Proposition 49**

Soit  $a$  et  $b$  deux entiers non nuls qui se décomposent en produits de facteurs premiers (distincts) de la façon suivante

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_r^{\beta_r}$$

où les  $\alpha_i$  et  $\beta_i$  sont des entiers éventuellement nuls. Alors

$$\text{ppcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \times p_2^{\max(\alpha_2, \beta_2)} \times \dots \times p_r^{\max(\alpha_r, \beta_r)}$$

**Proposition 50**

Soit de entiers  $a > 0$  et  $b > 0$ . Si  $d = \text{pgcd}(a, b)$  et  $m = \text{ppcm}(a, b)$ , alors  $ab = dm$ .

*Démonstration.* On remarque que pour  $x, y \in \mathbb{N}$ , on a  $x + y = \max(x, y) + \min(x, y)$ .

Il suffit alors de comparer les exposants de  $p$  dans  $ab$  et  $dm$  : ils sont égaux. ■

## 15.6 LA RELATION DE CONGRUENCE

### §1 La notion de congruence dans $\mathbb{Z}$

**Définition 51**

Soit  $a, b, n \in \mathbb{Z}$  trois entiers. On définit la relation de congruence par

$$(a \equiv b \pmod{n}) \iff (\exists k \in \mathbb{Z}, a = b + kn).$$

On dit que « $a$  est **congru** à  $b$  **modulo**  $n$ ». Les réels  $a$  et  $b$  diffèrent donc d'un multiple entier de  $n$  c'est-à-dire  $x - y \in n\mathbb{Z}$ .

**Proposition 52**

Soit  $n \in \mathbb{Z}$ . La relation de congruence modulo  $n$  est une relation d'équivalence sur  $\mathbb{Z}$ .

La classe d'équivalence de  $a \in \mathbb{Z}$  modulo  $n$  est

$$a + n\mathbb{Z} = \{ a + kn \mid k \in \mathbb{Z} \}.$$

### Exemple 53

- $230897 \equiv 7 \pmod{10}$ .
- $17 \equiv 2 \pmod{3}$ , mais aussi  $17 \equiv -1 \pmod{3}$ .

## §2 Lien avec la division euclidienne

### Proposition 54

Soit  $a, b, r \in \mathbb{Z}$ . Le reste de la division euclidienne de  $a$  par  $b$  est  $r$  si, et seulement si

$$a \equiv r \pmod{b} \quad \text{et} \quad 0 \leq r < b.$$

On a donc

$$b \mid a \iff a \equiv 0 \pmod{b}.$$

## §3 Compatibilité avec les opérations algébriques

### Proposition 55

Soient  $n \in \mathbb{Z}^*$ ,  $a, b, c, d, k \in \mathbb{Z}$  et  $p \in \mathbb{N}$ .

1. Si  $a \equiv b \pmod{n}$  et  $c \equiv d \pmod{n}$ , alors

$$a + c \equiv b + d \pmod{n}; \quad a - c \equiv b - d \pmod{n}; \quad ac \equiv bd \pmod{n}.$$

2. Si  $a \equiv b \pmod{n}$ , alors

$$ka \equiv kb \pmod{kn}; \quad ka \equiv kb \pmod{n}; \quad a^p \equiv b^p \pmod{n}$$

### Test 56

Démontrer la proposition précédente.

## §4 Équations du premier degré en congruence

Soit un entier  $n > 0$ , et  $a, b \in \mathbb{Z}$ . On cherche les entiers  $x \in \mathbb{Z}$  tels que

$$ax \equiv b \pmod{n}.$$

Tout revient à chercher  $x \in \mathbb{Z}$  pour lequel il existe  $y \in \mathbb{Z}$  tel que  $ax + ny = b$ . Ce problème a déjà été étudié et il admet des solutions si, et seulement si  $b$  est un multiple de  $\text{pgcd}(a, n)$ .

On se limite désormais au cas où  $a$  est premier avec  $n$ . L'égalité de Bézout permet d'introduire  $(u, v) \in \mathbb{Z}^2$  tel que

$$au + nv = 1.$$

On a  $au \equiv 1 \pmod{n}$  et on dit que  $u$  est **un inverse modulo  $n$**  de  $a$ . Il y a unicité de  $u$  si l'on décide que  $0 \leq u < n$ .

Pour résoudre  $ax \equiv b \pmod{n}$ , multiplions par  $u$ :

$$aux \equiv ub \pmod{n}, \text{ c'est-à-dire } x \equiv ub \pmod{n}.$$

Inversement, et en remultipliant par  $n$ , on trouve comme solution du problème tout entier congru à  $ub \pmod{n}$ .

### Exemple 57

Résoudre  $5x \equiv 9 \pmod{17}$ .

## §5 Théorème Chinois

### Théorème 58

#### Théorème Chinois

Soient  $m_1, \dots, m_r$  des entiers premiers entre eux deux à deux ( $m_i \geq 2$  et  $r \geq 2$ ) et  $M$  leur produit. Étant donnée des entiers  $a_1, \dots, a_r$ , considérons le système de congruences

$$\forall i \in \{1, \dots, r\}, x \equiv a_i \pmod{m_i}. \quad (S)$$

Ce système possède une solution  $x \in \mathbb{Z}$ , qui est unique modulo  $M$ .

*Démonstration.* Commençons par l'unicité. Soient  $x, y \in \mathbb{Z}$  deux solutions de  $(S)$ . Pour tout  $i$ ,  $x \equiv a_i \equiv y \pmod{m_i}$ , donc  $x - y$  est multiple de  $m_i$ . Ainsi,  $x - y$  est multiple du ppcm des  $m_i$  qui vaut  $M$  puisque les  $m_i$  sont premiers entre eux deux à deux. D'où  $x \equiv y \pmod{M}$ .

Pour l'existence, supposons que  $r = 2$ . Puisque  $m_1$  et  $m_2$  sont premiers entre eux, il existe  $u, v \in \mathbb{Z}$  tels que

$$um_1 + vm_2 = 1.$$

Posons  $x_1 = vm_2 = 1 - um_1$  et  $x_2 = um_1 = 1 - vm_2$ . Alors

$$\begin{aligned} x_1 &\equiv 1 \pmod{m_1}, & x_2 &\equiv 0 \pmod{m_1}, \\ x_1 &\equiv 0 \pmod{m_2}, & x_2 &\equiv 1 \pmod{m_2}. \end{aligned}$$

Posons  $x_0 = a_1x_1 + a_2x_2$ . Alors  $x_0$  est solution de  $(S)$ , ainsi que tout  $x \equiv x_0 \pmod{M}$ .

Pour le cas général, on effectue une récurrence sur  $r$ . ■

### Exemple 59

La preuve précédente fournit une méthode pratique de résolution du système. Résoudre par exemple

$$x \equiv 5 \pmod{17} \quad \text{et} \quad x \equiv 3 \pmod{23}. \quad (S)$$

Les nombre 17 et 23 étant premiers entre eux, il existe  $u, v \in \mathbb{Z}$  tels que  $17u + 23v = 1$ , par exemple  $(u, v) = (-4, 3)$  convient. On pose  $x_1 = 3 \times 23 = 69$  et  $x_2 = 17 \times (-4) = -68$ . D'où une solution de  $(S)$

$$x_0 = 5x_1 + 3x_2 = 5 \times 69 + 3 \times (-68) = 141.$$

Ensuite,

$$\begin{aligned}
 & x \equiv 5 \pmod{17} \quad \text{et} \quad x \equiv 3 \pmod{23} \\
 \Leftrightarrow & x \equiv x_0 \pmod{17} \quad \text{et} \quad x \equiv x_0 \pmod{23} \\
 \Leftrightarrow & 17 \mid (x - x_0) \quad \text{et} \quad 23 \mid (x - x_0) \\
 \Leftrightarrow & 391 \mid (x - x_0) \qquad \qquad \qquad \text{car } \text{pgcd}(17, 23) = 1.
 \end{aligned}$$

Les solutions de  $(S)$  sont donc les entiers

$$x = 141 + 391k \quad \text{avec} \quad k \in \mathbb{Z}.$$

## §6 Petit théorème de Fermat

### Théorème 60

#### Petit théorème de Fermat

Soit  $p$  un nombre premier. Si  $a \in \mathbb{Z}$  n'est pas multiple de  $p$ , on a

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Démonstration.* Supposons que  $a$  n'est pas divisible par  $p$  et notons

$$N = a \times 2a \times 3a \times \dots \times (p-1)a = (p-1)!a^{p-1}.$$

Pour tout entier  $k$ , notons  $r_k$  le reste de la division euclidienne de  $ka$  par  $p$ . Alors

$$N \equiv r_1 \times r_2 \times \dots \times r_{p-1} \pmod{p}.$$

Montrons que  $r_1, \dots, r_{p-1}$  sont tous distincts deux à deux. En effet, si  $r_i = r_j$ , alors  $(i-j)a$  est divisible par  $p$ , donc, en utilisant le lemme d'Euclide,  $(i-j)$  est aussi divisible par  $p$ . Or  $-p < i-j < p$ , on a donc nécessairement  $i = j$ .

De plus, en utilisant de nouveau le lemme d'Euclide, aucun  $ka$  n'est divisible par  $p$ , donc aucun  $r_k$  n'est nul. On en déduit alors que  $(r_1, r_2, \dots, r_{p-1})$  est une permutation de  $(1, 2, \dots, p-1)$  et donc

$$r_1 \times r_2 \times r_3 \times \dots \times r_{p-1} = (p-1)!$$

Finalement, on en déduit

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p},$$

autrement dit,  $(p-1)!(a^{p-1} - 1)$  est divisible par  $p$ . Puisque  $p$  est premier,  $p$  ne divise pas  $(p-1)!$  et le lemme d'Euclide assure alors que  $a^{p-1} - 1$  est divisible par  $p$ . ■

*Démonstration.* On peut également faire une démonstration par récurrence (voir en exercice). ■

Un énoncé équivalent est



**Théorème 61****Petit théorème de Fermat**

*Soit  $p$  un nombre premier et  $a \in \mathbb{Z}$ . On a*

$$a^p \equiv a \pmod{p}.$$