CHAPITRE 8

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

8.1 DIVISIBILITÉ ET DIVISION EUCLIDIENNE

§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 $D(b) = \left\{ a \in \mathbb{N} \,\middle|\, a \mid b \right\}$ l'ensemble des diviseurs positifs de b.

Exemples 2

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

$$\forall a \in \mathbb{Z}, a \mid 0 \text{ et } \left(0 \mid a \iff a = 0\right).$$

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 $\Big(a \mid b \text{ et } b \mid a\Big)$.

Proposition 7 **Caractérisation des couples d'intiers 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 algèbriques**

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

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

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

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

($\Longleftarrow$) 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, $a \mid b$.

∎

8.2 Les nombres premiers

§1 Définition

Définition 9 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 10 *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 11 **(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 12 *Soit $n > 1$. Si n n'est pas premier, il possède un facteur premier p tel que $p^2 \leq n$.*

Algorithme 13 **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.

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

§3 Ensemble des nombres premiers

Théorème 14 *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. ∎

8.3 Division euclidienne

§1 Division euclidienne

Définition 15 **Division euclidienne dans $\mathbb{Z}$**
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^\star$. Alors il existe un unique couple d'entiers $(q, r) \in \mathbb{Z} \times \mathbb{N}$ vérifiant

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

- 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 $a \mod b$..

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 16

543	17
33	31
16	

Ici $a = 543, b = 17, q = 31, r = 16$.

Proposition 17 *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 18 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 19

1. *Pour tout entier $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.*
2. *Réciproquement, soit A un sous-groupe de $\mathbb{Z}$, il existe un* unique *entier $n \geq 0$ tel que*
$$A = n\mathbb{Z}.$$

Proposition 20 *Soient A et B deux sous-groupes de $\mathbb{Z}$, alors la somme de ces deux sous-groupes*

$$A + B = \{\, a + b \mid a \in A \text{ et } b \in B \,\}$$

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

Proposition 21 *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 $\mathbb{Z}$.*

8.4 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*

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

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, $\text{pgcd}(a, b) = |a|$.

§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:

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

Théorème 26

Égalité de Bézout
Deux entiers a et b sont premiers entre eux si, et seulement si

$$\exists (u, v) \in \mathbb{Z}^2, ua + vb = 1.$$

Définition 27

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 ± 1.
- On dit que $a_1, \dots, a_r$ sont **premiers entre eux deux à deux** a_i et a_j sont premiers entre eux pour tous $i, j \in [\![1, r]\!]$ distincts.

§3 Lemme de Gauß, lemme d'Euclide

Théorème 28

Lemme de Gauß
Si a est premier avec b et a divise bc, alors a divise c.

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

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

∎

Théorème 29

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. ∎

On peut néanmoins une démonstration directe.

Démonstration. 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 30

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, $(n \in \mathbb{N}^\star)$, alors il divise a.*

Théorème 31

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 32

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* $r = a \mod b$.
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' et b' les entiers tels que $a=da'$ et $b=db'$. Alors d est le pgcd de a et b si, et seulement si, a' et b' sont premiers entre eux.*

Algorithme 33 **Algorithme d'Euclide**

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

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

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 34

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 35 **Algorithme d'Euclide étendu**

On peut supposer que $0\le b\le a$ 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 $(u_k)_{0\le k\le N}$ et $(v_k)_{0\le k\le N}$ par les relations

$$\begin{gathered}(u_0,v_0)=(1,0)\\(u_1,v_1)=(0,1)\\\forall k\in[\![0,N-2]\!],\left(u_{k+2},v_{k+2}\right)=\left(u_k-q_{k+2}u_{k+1},v_k-q_{k+2}v_{k+1}\right).\end{gathered}$$

On vérifie alors par récurrence que pour tout $k\in[\![0,N]\!]$,

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

En effet, on on a

$$\begin{aligned}r_0=a=a\times1+b\times0=au_0+bv_0\\\text{et }\ r_1=b=a\times0+b\times0=au_1+bv_1.\end{aligned}$$

D'où $H(0)$ et $H(1)$. Soit $k\in[\![0,N-2]\!]$. 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

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

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* $k \in [\![0, N]\!]$, *en particulier*

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

§5 Plus petit commun multiple de deux entiers

Définition 36

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 $\operatorname{ppcm}(a, b)$ ou $a \vee b$.

Théorème 37

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

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*

$$\operatorname{ppcm}(a, b) = \min\left\{ n \in \mathbb{N}^\star \;\middle|\; a \,\middle|\, n \text{ et } b \,\middle|\, n \right\}.$$

§6 Généralisation

Définition 38

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

- On appelle **plus grand commun diviseur** de $a_1, \ldots, a_r$ l'unique entier naturel d pour lequel
$$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_r\mathbb{Z} = d\mathbb{Z}.$$
-
- On appelle **plus petit commun multiple** de $a_1, \ldots, a_r$ l'unique entier naturel m pour lequel
$$a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \cdots \cap a_r\mathbb{Z} = m\mathbb{Z}.$$

8.5 Décomposition en facteurs premiers

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

Théorème 39 **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

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

Exemple 40 $90 = 9 \times 10 = 3 \times 3 \times 2 \times 5 = 2 \times 3 \times 3 \times 5 = 2 \times 3^2 \times 5.$

§2 Valuation p-adique

Définition 41 La décomposition de $n \geq 2$ en facteurs premiers peut également s'écrire sous la forme

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

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 α_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.

Proposition 42 *Soit $a, b \in \mathbb{N}^\star$, et $p \in \mathbb{P}$. On a*

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

Proposition 43 *Soit $a, b \in \mathbb{N}^\star$, alors $a \mid b$ si, et seulement si*

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

Proposition 44 *Soit n un entier non nul qui se décompose en produit de facteurs premiers (distincts) de la façon suivante*

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

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

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

Test 45 Quels sont les diviseurs de 90?

§3 Applications

Proposition 46 *Soit a et b deux entiers non nuls qui se décomposent en produits de facteurs premiers (distincts) de la façon suivante*

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

où les α_i et β_i sont des entiers éventuellement nuls. Alors

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

Test 47 Retrouver le pgcd de 105 et 48.

Proposition 48 *Soit a et b deux entiers non nuls qui se décomposent en produits de facteurs premiers (distincts) de la façon suivante*

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

où les α_i et β_i sont des entiers éventuellement nuls. Alors

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

Proposition 49 *Soit de entiers $a > 0$ et $b > 0$. Si $d = \operatorname{pgcd}(a, b)$ et $m = \operatorname{ppcm}(a, b)$, 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. ∎

8.6 La relation de congruence

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

Définition 50

Soit $a, b, n \in Z$ trois entiers. On défini 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 $x - y \in n\mathbb{Z}$.

Exemple 51

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

Notation

Pour tous entiers a et n, on note $a + n\mathbb{Z}$ l'ensemble des entiers congrus à a modulo n. Ce sont les entiers de la forme $a + kn$, où $k \in \mathbb{Z}$. On note

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

Exemple 52

L'ensemble des nombres impairs peut donc se noter $1 + 2\mathbb{Z}$; celui des nombres donc l'écriture décimale termine par 5 peut se noter $5 + 10\mathbb{Z}$.

§2 Lien avec la division euclidienne

Proposition 53

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

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

On a donc

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

§3 Compatibilité avec les opérations algébriques

Proposition 54

Soient $n \in \mathbb{Z}^\star$, $a, b, c, d, k \in \mathbb{Z}$ 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 55 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 56 Résoudre $5x \equiv 9 \pmod{17}$.

§5 Petit théorème de Fermat

Théorème 57

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

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

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

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

Montrons que $r_1, \ldots, r_{p-1}$ 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 $(r_1, r_2, \ldots, r_{p-1})$ est une permutation de $(1, 2, \ldots, p-1)$ et donc

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

Finalement, on en déduit

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

autrement dit, $(p-1)!\left(a^{p-1} - 1\right)$ 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 58 **Petit théorème de Fermat**
Soit p un nombre premier et $a \in \mathbb{Z}$. On a

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