UNIVERSITÉ MOHAMMED V

FACULTÉ DES SCIENCES DE RABAT

Département de Mathématiques

FORMATION UNIVERSITAIRE

Licence – Sciences Mathématiques

Algèbre I

CHAPITRE 3

Arithmétique dans $\mathbb{Z}$

Divisibilité, congruences et nombres premiers

SUPPORT DE COURS

Prof. Mohamed Najib LAATABI

najib.laatabi@um5r.ac.ma

mohamednajiblaatabi.com

Toute remarque ou suggestion est la bienvenue. Si vous constatez une erreur dans ce document, merci de bien vouloir la signaler.

Année universitaire • **2026–2027**

Sommaire du chapitre

Notations et symboles **ii**

3 Arithmétique dans $\mathbb{Z}$ **1**
3.1 Division euclidienne, diviseur et multiple . . . 1
3.1.1 Division euclidienne dans $\mathbb{N}$ et dans $\mathbb{Z}$ . . . 1
3.1.2 Notion de diviseur commun . . . 3
3.1.3 Plus grand commun diviseur : pgcd . . . 3
3.1.4 Plus petit commun multiple : ppcm . . . 4
3.1.5 Lemme d'Euclide : invariance du PGCD . . . 4
3.1.6 Algorithme d'Euclide . . . 5
3.2 Théorème de Bézout et ses corollaires . . . 5
3.2.1 Algorithme d'Euclide étendu et identité de Bézout . . . 5
3.2.2 Théorème de Bézout . . . 6
3.2.3 Théorème de Gauss . . . 8
3.2.4 Résolution des équations diophantiennes . . . 8
3.3 Congruences et arithmétique modulaire . . . 9
3.3.1 Congruence modulo un entier . . . 9
3.3.2 Compatibilité de la congruence avec les opérations usuelles . . . 10
3.3.3 Petit théorème de Fermat . . . 11
3.3.4 L'anneau quotient $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ . . . 12
3.4 Notion de primalité dans $\mathbb{N}$ et dans $\mathbb{Z}$ . . . 13
3.4.1 Nombres premiers . . . 13
3.4.2 Théorème fondamental de l'arithmétique . . . 14
3.5 Fonction indicatrice d'Euler . . . 16

Références bibliographiques **18**

Notations et symboles

Symbole	Signification
Ensembles et logique	
$\mathbb{N},\ \mathbb{N}^*$	Entiers naturels (avec 0) ; entiers naturels strictement positifs
$\mathbb{Z},\ \mathbb{Z}^*$	Entiers relatifs ; entiers relatifs non nuls
$\mathbb{P}$	Ensemble des nombres premiers positifs : $\{2, 3, 5, 7, \ldots\}$
$\forall,\ \exists,\ \exists!$	Pour tout ; il existe ; il existe un unique
$P \implies Q,\ P \iff Q$	Implication ; équivalence logique
$\in,\ \notin,\ \subseteq$	Appartient ; n'appartient pas ; est inclus dans
$A \cap B,\ A \setminus B$	Intersection ; différence ensembliste
$\lvert a \rvert$	Valeur absolue de l'entier a
$\mathrm{Card}(E)$	Nombre d'éléments d'un ensemble fini E
Divisibilité, PGCD et PPCM	
$b \mid a,\ b \nmid a$	b divise a ; b ne divise pas a
$a = bq + r$	Division euclidienne : $b \neq 0$, $q \in \mathbb{Z}$ et $0 \leq r < \lvert b \rvert$
D_a	Ensemble des diviseurs relatifs de a : $\{d \in \mathbb{Z} : d \mid a\}$
$\mathcal{D}_p$	Ensemble des diviseurs strictement positifs de p
$M_a = a\mathbb{Z}$	Ensemble des multiples de a : $\{ak : k \in \mathbb{Z}\}$
$\mathrm{pgcd}(a, b)$	Plus grand commun diviseur de a et b ; par convention, $\mathrm{pgcd}(0, 0) = 0$
$\mathrm{ppcm}(a, b)$	Plus petit commun multiple positif si $ab \neq 0$; vaut 0 si $ab = 0$
$au + bv = \mathrm{pgcd}(a, b)$	Identité de Bézout, avec $u, v \in \mathbb{Z}$
$\mathrm{pgcd}(a, b) = 1$	Les entiers a et b sont premiers entre eux
Congruences, classes et primalité	
$a \equiv b \pmod{n}$	Congruence modulo n : $n \mid a - b$; également notée $a \equiv b\ [n]$
$\overline{a} = a + n\mathbb{Z}$	Classe de congruence de a modulo n
$\mathbb{Z}/n\mathbb{Z}$	Ensemble des classes de congruence modulo n
$(\mathbb{Z}/n\mathbb{Z})^\times$	Groupe des classes inversibles modulo n, pour $n \geq 2$
$\overline{a}^{-1}$	Inverse multiplicatif de la classe $\overline{a}$, lorsqu'il existe
$\mathbb{Z}[X]$	Ensemble des polynômes à coefficients entiers
$n!,\ \binom{n}{k}$	Factorielle ($0! = 1$) ; coefficient binomial
$\prod_{i=1}^{r} p_i^{\alpha_i}$	Produit de puissances de nombres premiers
$\varepsilon \in \{-1, 1\}$	Signe d'un entier non nul : $\varepsilon = a/\lvert a \rvert$
$\phi(n)$	Indicatrice d'Euler : nombre d'entiers $a \in \{1, \ldots, n\}$ premiers avec n ; $\phi(1) = 1$

Chapitre 3

Arithmétique dans $\mathbb{Z}$

3.1 Division euclidienne, diviseur et multiple

3.1.1 Division euclidienne dans $\mathbb{N}$ et dans $\mathbb{Z}$

Théorème 3.1.1 – Division euclidienne dans $\mathbb{N}$

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que

$$a = bq + r, \qquad 0 \leq r < b.$$

Démonstration. **Existence.** L'ensemble $E = \{k \in \mathbb{N} : a < bk\}$ est non vide par la propriété d'Archimède. Soit $m = \min E$. Puisque $a \geq 0$, on a $m \geq 1$ et

$$(m-1)b \leq a < mb.$$

En posant $q = m - 1$ et $r = a - bq$, on obtient $a = bq + r$ et $0 \leq r < b$.

Unicité. Si $a = bq + r = bq' + r'$ avec $0 \leq r, r' < b$, alors $b(q - q') = r' - r$. Or $|r' - r| < b$, donc $|q - q'| < 1$. Ainsi $q = q'$ et $r = r'$. ■

Exemple 1

$$159 = 11 \times 14 + 5, \qquad 0 \leq 5 < 11.$$

Le quotient est 14 et le reste est 5.

Théorème 3.1.2 – Division euclidienne dans $\mathbb{Z}$

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$\boxed{a = bq + r, \qquad 0 \leq r < |b|.}$$

Démonstration. Posons $c = |b| > 0$. Si $a \geq 0$, la division dans $\mathbb{N}$ donne $a = cq_0 + r$ avec $0 \leq r < c$. Si $a < 0$, écrivons $-a = cq_0 + r_0$, avec $0 \leq r_0 < c$.

i) Si $r_0 = 0$, alors $a = c(-q_0) + 0$.

ii) Si $r_0 > 0$, alors $a = c(-q_0 - 1) + (c - r_0)$ et $0 < c - r_0 < c$.

On obtient dans tous les cas $a = cQ + r$ avec $Q \in \mathbb{Z}$ et $0 \leq r < c$. On prend $q = Q$ si $b > 0$, et $q = -Q$ si $b < 0$.

Si $a = bq + r = bq' + r'$, alors $|b|\,|q - q'| = |r' - r| < |b|$. Donc $q = q'$ et $r = r'$. ■

Exemple 2

$$-159 = 11(-15) + 6, \qquad 159 = (-11)(-14) + 5,$$
$$-159 = (-11)(15) + 6, \quad -154 = 11(-14) + 0.$$

Dans chaque cas, le reste appartient à $\{0, 1, \ldots, 10\}$.

Définition 3.1.1

Soient $a, b \in \mathbb{Z}$. On dit que b divise a, ou que a est un multiple de b, lorsque

$$\boxed{b \mid a \iff \exists q \in \mathbb{Z},\ a = bq.}$$

Lorsque $b \neq 0$, cela équivaut à la nullité du reste de la division euclidienne de a par b.

Exemple 3

$$176 = 16 \times 11, \qquad -176 = 16(-11) = (-16)11.$$

Ainsi $16 \mid 176$, $11 \mid 176$, $16 \mid -176$ et $-16 \mid -176$.

Remarque 1

Pour tous $a, b, n \in \mathbb{Z}$:

i) $a \mid 0$, y compris lorsque $a = 0$; en particulier $0 \mid 0$.

ii) $0 \mid a$ si et seulement si $a = 0$.

iii) $1 \mid a$ et $-1 \mid a$.

iv) $b \mid a \iff |b| \mid |a|$.

v) Si $n \mid a$ et $n \mid b$, alors
$$\forall (\lambda, \mu) \in \mathbb{Z}^2, \quad n \mid \lambda a + \mu b.$$

vi) Si $b \mid a$ et $a \neq 0$, alors $b \neq 0$ et $|b| \leq |a|$.

Remarque 2

La divisibilité est réflexive et transitive sur $\mathbb{Z}$:

$$a \mid a, \qquad (a \mid b \text{ et } b \mid c) \Longrightarrow a \mid c.$$

De plus,
$$(a \mid b \text{ et } b \mid a) \iff |a| = |b| \iff b = a \text{ ou } b = -a.$$

Elle est donc un ordre partiel sur $\mathbb{N}$, mais seulement un préordre sur $\mathbb{Z}$. Elle n'est pas antisymétrique sur $\mathbb{Z}$ car $2 \mid -2$ et $-2 \mid 2$. Elle n'est pas symétrique : $2 \mid 4$ tandis que $4 \nmid 2$.

3.1.2 Notion de diviseur commun

Définition 3.1.2
Soient $a, b \in \mathbb{Z}$. Un entier $d \in \mathbb{Z}$ est un diviseur commun de a et b lorsque

$$d \mid a \text{ et } d \mid b \iff \exists (k, k') \in \mathbb{Z}^2,\ a = kd,\ b = k'd.$$

Exemple 4
3 et -3 divisent 12 et -21 ; 7 et -7 divisent -14 et 21.

Remarque 3 – Combinaisons linéaires

$$d \mid a \text{ et } d \mid b \Longrightarrow \forall (\lambda, \mu) \in \mathbb{Z}^2, \quad d \mid \lambda a + \mu b.$$

En effet, $a = kd$ et $b = k'd$ donnent $\lambda a + \mu b = (\lambda k + \mu k')d$.

3.1.3 Plus grand commun diviseur : pgcd

Propriété 3.1.1 – Ensemble des diviseurs communs
Pour $a \in \mathbb{Z}$, posons $D_a = \{d \in \mathbb{Z} : d \mid a\}$.

i) Si $a \neq 0$, D_a est fini et $\max D_a = |a|$.

ii) $D_0 = \mathbb{Z}$.

iii) Si $(a, b) \neq (0, 0)$, $D_a \cap D_b$ est fini et contient -1 et 1. En outre,

$$1 \leq \max(D_a \cap D_b) \leq \max(|a|, |b|).$$

Définition 3.1.3
Pour $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, on définit

$$\operatorname{pgcd}(a, b) = \max(D_a \cap D_b).$$

Le PGCD est donc strictement positif. On pose par convention $\operatorname{pgcd}(0, 0) = 0$; cette convention ne provient pas d'un maximum de D_0.

Propriété 3.1.2
Pour tous $a, b \in \mathbb{Z}$,

$$\operatorname{pgcd}(a, b) = \operatorname{pgcd}(|a|, |b|) = \operatorname{pgcd}(b, a),$$
$$\operatorname{pgcd}(a, 0) = |a|, \qquad \operatorname{pgcd}(a, a) = |a|, \qquad \operatorname{pgcd}(a, 1) = 1.$$

Exemple 5

$$D_{-36} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 18, \pm 36\},$$
$$D_{30} = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}.$$

Ainsi $D_{-36} \cap D_{30} = \{-6, -3, -2, -1, 1, 2, 3, 6\}$ et

$$\text{pgcd}(-36, 30) = \text{pgcd}(36, -30) = 6.$$

3.1.4 Plus petit commun multiple : ppcm

Propriété 3.1.3 – Ensemble des multiples communs
Pour $a \in \mathbb{Z}$, l'ensemble de ses multiples est $M_a = a\mathbb{Z} = \{ak : k \in \mathbb{Z}\}$. Si $a, b \neq 0$, l'ensemble

$$M_a \cap M_b \cap \mathbb{N}^*$$

est non vide, car il contient $|ab|$. Il admet donc un plus petit élément.

Définition 3.1.4
Pour $a, b \in \mathbb{Z} \setminus \{0\}$, on définit

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

Si $ab = 0$, on pose $\text{ppcm}(a, b) = 0$. Ainsi, pour tous $a, b \in \mathbb{Z}$,

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

Remarque 4
Pour $a, b \neq 0$, on a

$$\max(|a|, |b|) \leq \text{ppcm}(a, b) \leq |ab|.$$

Le nombre 0 est toujours un multiple commun ; on l'exclut donc lors de la recherche du plus petit multiple commun *strictement positif*.

Exemple 6

$$M_{-42} \cap \mathbb{N}^* = \{42, 84, 126, 168, 210, 252, 294, 336, \ldots\},$$
$$M_{48} \cap \mathbb{N}^* = \{48, 96, 144, 192, 240, 288, 336, \ldots\}.$$

Donc $\text{ppcm}(-42, 48) = 336$ et $\text{ppcm}(-42, 0) = 0$.

3.1.5 Lemme d'Euclide : invariance du PGCD

Lemme 3.1.1
Pour tous $a, b, q \in \mathbb{Z}$,

$$D_a \cap D_b = D_{a-qb} \cap D_b, \qquad \boxed{\text{pgcd}(a, b) = \text{pgcd}(a - qb, b).}$$

Démonstration. Si $d \mid a$ et $d \mid b$, alors $d \mid a - qb$. Réciproquement, si $d \mid a - qb$ et $d \mid b$, alors $d \mid (a - qb) + qb = a$. Les ensembles de diviseurs communs sont égaux. Leurs maxima sont donc égaux lorsque $(a, b) \neq (0, 0)$; le cas $(a, b) = (0, 0)$ résulte de la convention adoptée. ■

Remarque 5

En particulier,

$$\operatorname{pgcd}(a,b) = \operatorname{pgcd}(a-b,b) = \operatorname{pgcd}(a+b,b).$$

Si $b \neq 0$ et $a = bq + r$ avec $0 \leq r < |b|$, alors

$$\operatorname{pgcd}(a,b) = \operatorname{pgcd}(b,r).$$

3.1.6 Algorithme d'Euclide

Soient $a, b \in \mathbb{Z}$, non tous deux nuls. Si $b = 0$, le PGCD vaut $|a|$. Sinon, posons $r_{-1} = |a|$ et $r_0 = |b| > 0$ et effectuons les divisions successives

$$r_{j-1} = q_j r_j + r_{j+1}, \qquad 0 \leq r_{j+1} < r_j,$$

tant que $r_j \neq 0$. Les restes positifs sont strictement décroissants ; il existe donc $s \geq 0$ tel que $r_s > 0$ et $r_{s+1} = 0$. L'invariance du PGCD donne

$$\operatorname{pgcd}(a,b) = \operatorname{pgcd}(r_{-1}, r_0) = \cdots = \operatorname{pgcd}(r_s, 0) = r_s.$$

Le PGCD est le dernier terme non nul de l'algorithme, y compris le diviseur initial si la première division a un reste nul.

Exemple 7

$$72 = 2 \times 30 + 12, \qquad 30 = 2 \times 12 + 6, \qquad 12 = 2 \times 6.$$

Ainsi $\operatorname{pgcd}(72, 30) = \operatorname{pgcd}(-72, 30) = 6$.

3.2 Théorème de Bézout et ses corollaires

3.2.1 Algorithme d'Euclide étendu et identité de Bézout

Théorème 3.2.1 – Identité de Bachet–Bézout

Pour tous $a, b \in \mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tels que

$$\boxed{au + bv = \operatorname{pgcd}(a,b).}$$

Démonstration. Si $a = b = 0$, prendre $u = v = 0$. Si $b = 0$ et $a \neq 0$, prendre $u = a/|a|$ et $v = 0$; le cas $a = 0$ se traite de même.

Supposons $a, b \neq 0$. Dans l'algorithme d'Euclide appliqué à $|a|, |b|$, chaque reste est une combinaison linéaire entière de $|a|$ et $|b|$. En effet, c'est vrai pour les deux termes initiaux, puis

$$r_{j+1} = r_{j-1} - q_j r_j$$

conserve cette propriété. Pour le dernier reste non nul d, il existe $U, V \in \mathbb{Z}$ tels que $d = U|a| + V|b|$. En posant $u = U\, a/|a|$ et $v = V\, b/|b|$, on obtient $d = au + bv$. ∎

Remarque 6 – Calcul des coefficients
Dans l'algorithme sur $|a|, |b|$, on peut calculer simultanément

$$(u_{-1}, v_{-1}) = (1, 0), \qquad (u_0, v_0) = (0, 1),$$
$$u_{j+1} = u_{j-1} - q_j u_j, \qquad v_{j+1} = v_{j-1} - q_j v_j.$$

Alors $r_j = u_j|a| + v_j|b|$. Les coefficients correspondant au dernier reste non nul fournissent l'identité de Bézout, après prise en compte des signes de a et b.

Exemple 8

$$564 = 27 \times 20 + 24, \qquad 27 = 24 + 3, \qquad 24 = 3 \times 8.$$

Donc $\text{pgcd}(564, 27) = 3$ et

$$3 = 27 - 24 = 27 - (564 - 20 \times 27) = -564 + 21 \times 27.$$

Pour les entiers -564 et 27, on obtient

$$3 = 1 \times (-564) + 21 \times 27.$$

Corollaire 3.2.1
Pour tous $a, b, c \in \mathbb{Z}$,

$$\exists (u, v) \in \mathbb{Z}^2,\ au + bv = c \quad \Longleftrightarrow \quad \text{pgcd}(a, b) \mid c.$$

Démonstration. Tout diviseur commun de a et b divise $au + bv$. Réciproquement, si $c = kd$ avec $d = \text{pgcd}(a, b)$ et $d = au_0 + bv_0$, alors $c = a(ku_0) + b(kv_0)$. Le cas $d = 0$ correspond à $a = b = c = 0$. ■

Remarque 7
L'égalité $au + bv = c$ n'implique pas que c soit le PGCD. Par exemple,

$$24 = 6 \times 5 + 2 \times (-3), \qquad \text{pgcd}(6, 2) = 2.$$

3.2.2 Théorème de Bézout

Définition 3.2.1
Deux entiers $a, b \in \mathbb{Z}$ sont premiers entre eux lorsque $\text{pgcd}(a, b) = 1$.

Remarque 8 – Caractérisation par les diviseurs
Avec $D_a = \{d \in \mathbb{Z} : d \mid a\}$,

$$a, b \text{ premiers entre eux} \Longleftrightarrow D_a \cap D_b = \{-1, 1\}.$$

Si l'on considère seulement les diviseurs positifs, l'intersection est alors $\{1\}$. En particulier, 0 est premier avec b si et seulement si $b \in \{-1, 1\}$.

Propriété 3.2.1

Si $(a,b) \neq (0,0)$, les conditions suivantes sont équivalentes :

i) a et b ne sont pas premiers entre eux ;

ii) $\text{pgcd}(a,b) > 1$;

iii) il existe $d \geq 2$ tel que $d \mid a$ et $d \mid b$;

iv) $\text{Card}(D_a \cap D_b) > 2$.

Démonstration. Le PGCD est positif et appartient à $D_a \cap D_b$. Si ce PGCD dépasse 1, ses deux signes s'ajoutent aux diviseurs ± 1. Réciproquement, un diviseur commun autre que ± 1 a une valeur absolue au moins égale à 2 et minore le PGCD. ■

Remarque 9

Les entiers 0 et 0 ne sont pas premiers entre eux et tout $d \geq 2$ les divise ; leur PGCD vaut cependant 0 par convention.

Théorème 3.2.2 – Théorème de Bézout

Pour tous $a, b \in \mathbb{Z}$,

$$\boxed{\text{pgcd}(a,b) = 1 \iff \exists (u,v) \in \mathbb{Z}^2,\ au + bv = 1.}$$

On peut remplacer 1 par -1 dans le second membre.

Démonstration. Le sens direct résulte de l'identité de Bézout. Réciproquement, si $au+bv = 1$, le PGCD divise 1 ; étant positif, il vaut 1. Enfin, $au+bv = 1$ équivaut à $a(-u)+b(-v) = -1$. ■

Exemple 9

Pour tout $n \in \mathbb{Z}$,

$$-n + (n+1) = 1, \qquad -2n + (2n+1) = 1.$$

Donc $\text{pgcd}(n, n+1) = \text{pgcd}(n, 2n+1) = 1$.

Remarque 10

Pour tous $a, b \in \mathbb{Z}$,

$$\text{pgcd}(a,b) \neq 1 \iff \forall (u,v) \in \mathbb{Z}^2,\ au + bv \neq 1.$$

Corollaire 3.2.2

Pour tous $a, m, n \in \mathbb{Z}$,

$$\Big(\text{pgcd}(a,m) = 1 \text{ et } \text{pgcd}(a,n) = 1\Big) \iff \text{pgcd}(a, mn) = 1.$$

Démonstration. Si $au + mv = 1$ et $as + nt = 1$, alors

$$1 = (au + mv)(as + nt) = a(aus + unt + mvs) + mnvt.$$

Le théorème de Bézout donne $\text{pgcd}(a, mn) = 1$. Réciproquement, si $au + mnv = 1$, cette identité est à la fois une identité de Bézout pour (a, m) et pour (a, n). ■

3.2.3 Théorème de Gauss

Théorème 3.2.3 – Théorème de Gauss

Pour tous $a, b, c \in \mathbb{Z}$,

$$c \mid ab \text{ et } \operatorname{pgcd}(c, a) = 1 \quad \Longrightarrow \quad c \mid b.$$

Démonstration. Par Bézout, il existe $u, v \in \mathbb{Z}$ tels que $uc + va = 1$. Alors $b = ubc + vab$. Les deux termes de droite sont divisibles par c, donc $c \mid b$. ■

Corollaire 3.2.3 – Relation entre PGCD et PPCM

Pour tous $a, b \in \mathbb{Z}$,

$$\boxed{\operatorname{pgcd}(a, b)\operatorname{ppcm}(a, b) = |ab|.}$$

Démonstration. Si $ab = 0$, les deux membres sont nuls. Sinon, posons $d = \operatorname{pgcd}(a, b)$, $|a| = dA$, $|b| = dB$ avec $A, B > 0$. En divisant une identité de Bézout par d, on obtient $\operatorname{pgcd}(A, B) = 1$.

Le nombre dAB est un multiple commun positif. Si $m > 0$ est un autre multiple commun, écrivons $m = dAk$. Comme $dB \mid m$, on a $B \mid Ak$. Par Gauss, $B \mid k$, donc $dAB \mid m$. Ainsi $\operatorname{ppcm}(a, b) = dAB = |ab|/d$. ■

3.2.4 Résolution des équations diophantiennes

Théorème 3.2.4 – Équation diophantienne linéaire

Soient $a, b, c \in \mathbb{Z}$ avec $(a, b) \neq (0, 0)$ et $d = \operatorname{pgcd}(a, b) > 0$. L'équation $ax + by = c$ admet une solution dans $\mathbb{Z}^2$ si et seulement si $d \mid c$. Dans ce cas, si (x_0, y_0) est une solution, toutes les solutions sont

$$\boxed{(x, y) = \left(x_0 + \frac{b}{d}k,\ y_0 - \frac{a}{d}k\right), \qquad k \in \mathbb{Z}.}$$

Démonstration. La condition d'existence a été démontrée. Si $au + bv = d$, une solution particulière est $(x_0, y_0) = (cu/d, cv/d)$.

Supposons d'abord $a, b \neq 0$ et posons $a' = a/d$, $b' = b/d$. Deux solutions vérifient

$$a'(x - x_0) = -b'(y - y_0), \qquad \operatorname{pgcd}(a', b') = 1.$$

Par Gauss, $a' \mid y - y_0$. Écrivons $y - y_0 = -a'k$; alors $x - x_0 = b'k$ puisque $a' \neq 0$. Réciproquement, ces couples satisfont l'équation.

Si $a = 0$ et $b \neq 0$, on a $y = c/b$ et x arbitraire ; la formule reste valable car $b/d = \pm 1$. Le cas $b = 0$ est analogue. ■

Remarque 11

Si $a = b = 0$, l'équation admet toutes les paires de $\mathbb{Z}^2$ lorsque $c = 0$, et aucune solution lorsque $c \neq 0$.

Exemple 10

i) Les solutions de $3x + 7y = 11$ sont $(x, y) = (6 + 7k, -1 - 3k)$, $k \in \mathbb{Z}$.

ii) Les solutions de $-3x + 7y = 11$ sont $(x, y) = (-6 + 7k, -1 + 3k)$, $k \in \mathbb{Z}$.

iii) Pour tout $a \in \mathbb{Z}$, l'équation $303x + 57y = a^2 + 1$ n'a pas de solution entière : $\text{pgcd}(303, 57) = 3$ et $a^2 \equiv 0$ ou $1 \pmod 3$, donc $3 \nmid a^2 + 1$.

3.3 Congruences et arithmétique modulaire

3.3.1 Congruence modulo un entier

Définition 3.3.1

Soit $n \in \mathbb{Z}$. Pour $a, b \in \mathbb{Z}$, on définit

$$a \equiv b \pmod n \iff n \mid a - b \iff \exists k \in \mathbb{Z},\ a - b = kn.$$

On note également cette congruence $a \equiv b\ [n]$.

Remarque 12

i) Pour $n \neq 0$, $a \equiv b \pmod n \iff a \equiv b \pmod{|n|}$.

ii) Modulo 1 ou -1, tous les entiers sont congrus entre eux.

iii) Modulo 0, la congruence est l'égalité : $a \equiv b \pmod 0 \iff a = b$.

Pour les résultats sur les anneaux quotients finis, on prendra $n \geq 2$.

Exemple 11

$$12 \equiv 7 \pmod 5, \qquad -3 \equiv 1 \pmod 4, \qquad -3 \equiv 1 \pmod{-4}.$$

En effet, $12 - 7 = 5$ et $-3 - 1 = -4$.

Proposition 3.3.1

Pour tous $a, n \in \mathbb{Z}$,

$$a \equiv 0 \pmod n \iff n \mid a.$$

Démonstration. Il suffit d'appliquer la définition à $a - 0 = a$. ■

Proposition 3.3.2

Soient $n \in \mathbb{Z} \setminus \{0\}$ et $a, b \in \mathbb{Z}$. Les entiers a et b sont congrus modulo n si et seulement si leurs restes dans la division euclidienne par n sont égaux.

Démonstration. Écrivons $a = nq_1 + r_1$ et $b = nq_2 + r_2$ avec $0 \leq r_1, r_2 < |n|$. Alors

$$n \mid a - b \iff n \mid r_1 - r_2.$$

Or $|r_1 - r_2| < |n|$, donc $n \mid r_1 - r_2$ équivaut à $r_1 = r_2$. ■

Proposition 3.3.3
Pour tout $n \in \mathbb{Z}$, la congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Démonstration. i) $a - a = 0 = n \times 0$, donc $a \equiv a \pmod{n}$.
ii) Si $a - b = kn$, alors $b - a = (-k)n$.
iii) Si $a - b = kn$ et $b - c = \ell n$, alors $a - c = (k + \ell)n$. ■

Remarque 13
La classe de a modulo n est

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

En particulier, $\overline{0} = n\mathbb{Z}$. Par exemple,

$$\overline{3} = \{\ldots, -18, -11, -4, 3, 10, 17, 24, \ldots\} = \overline{10} \quad \text{modulo } 7,$$
$$\overline{3} = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\} = \overline{13} \quad \text{modulo } 5.$$

Si $n \neq 0$, chaque classe possède un unique représentant dans $\{0, 1, \ldots, |n| - 1\}$. Ainsi

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{|n| - 1}\}.$$

Les éléments du quotient sont les *classes*, et non leurs représentants.

3.3.2 Compatibilité de la congruence avec les opérations usuelles

Proposition 3.3.4
Soient $n, a, b, a', b' \in \mathbb{Z}$. Si $a \equiv b \pmod{n}$ et $a' \equiv b' \pmod{n}$, alors

$$a + a' \equiv b + b' \pmod{n}, \qquad a - a' \equiv b - b' \pmod{n}, \qquad aa' \equiv bb' \pmod{n}.$$

Démonstration. Écrivons $a = b + kn$ et $a' = b' + k'n$. On obtient

$$(a \pm a') - (b \pm b') = (k \pm k')n, \qquad aa' - bb' = (bk' + kb' + kk'n)n.$$

■

Corollaire 3.3.1
Pour $a, b, n \in \mathbb{Z}$ et $r \in \mathbb{N}^*$,

$$a \equiv b \pmod{n} \quad \Longrightarrow \quad a^r \equiv b^r \pmod{n}.$$

Plus généralement, pour tout $P \in \mathbb{Z}[X]$, $a \equiv b \pmod{n}$ implique $P(a) \equiv P(b) \pmod{n}$.

Démonstration. La première assertion se démontre par récurrence sur r ; la seconde résulte de la compatibilité avec les sommes et les produits. ■

Exemple 12 – Divisibilité de $10^{1\,000\,000}+10$ par 13

$$\begin{aligned} 10 &\equiv -3 \pmod{13},\\ 10^3 &\equiv -27 \equiv -1 \pmod{13},\\ 10^{999\,999} &= (10^3)^{333\,333} \equiv -1 \pmod{13},\\ 10^{1\,000\,000}+10 &\equiv -10+10 \equiv 0 \pmod{13}. \end{aligned}$$

Proposition 3.3.5

Pour tous $m, n, a, b \in \mathbb{Z}$,

$$a \equiv b \pmod{mn} \implies \begin{cases} a \equiv b \pmod{m},\\ a \equiv b \pmod{n}. \end{cases}$$

Démonstration. Si $a-b=kmn$, alors $a-b=(kn)m=(km)n$. ■

Corollaire 3.3.2

$$a \not\equiv b \pmod{m} \implies a \not\equiv b \pmod{mn}.$$

3.3.3 Petit théorème de Fermat

Théorème 3.3.1 – Petit théorème de Fermat

Soit $p \geq 2$ un nombre premier. Pour tout $a \in \mathbb{Z}$,

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

Si de plus $\operatorname{pgcd}(a,p)=1$, alors

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

Lemme 3.3.1

Si p est premier et $1 \leq k \leq p-1$, alors $p \mid \binom{p}{k}$.

Démonstration. On a $k\binom{p}{k} = p\binom{p-1}{k-1}$. Les seuls diviseurs positifs de p sont 1 et p, et $p \nmid k$; ainsi $\operatorname{pgcd}(p,k)=1$. Le théorème de Gauss donne le résultat. ■

Démonstration du petit théorème de Fermat. Pour $r=0$, l'égalité $r^p \equiv r \pmod{p}$ est immédiate. Le binôme de Newton et le lemme précédent donnent

$$(r+1)^p \equiv r^p + 1 \pmod{p}.$$

Une récurrence établit donc $r^p \equiv r \pmod{p}$ pour $r \in \{0,\dots,p-1\}$.

Pour un entier relatif quelconque a, la division euclidienne donne $a=pq+r$, avec $q \in \mathbb{Z}$ et $0 \leq r < p$. Par compatibilité,

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

Enfin, si $\text{pgcd}(a,p)=1$, la divisibilité $p \mid a(a^{p-1}-1)$ et le théorème de Gauss entraînent $p \mid a^{p-1}-1$. ■

3.3.4 L'anneau quotient $(\mathbb{Z}/n\mathbb{Z},+,\times)$

Soit $n \geq 2$. On a

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0},\overline{1},\ldots,\overline{n-1}\}.$$

Les opérations sont définies, pour $a,b \in \mathbb{Z}$, par

$$\overline{a}+\overline{b}=\overline{a+b}, \qquad \overline{a}\,\overline{b}=\overline{ab}.$$

Elles ne dépendent pas du choix des représentants, par compatibilité de la congruence avec l'addition et la multiplication.

Propriété 3.3.1

L'ensemble $\mathbb{Z}/n\mathbb{Z}$, muni de ces opérations, est un anneau commutatif unitaire :

i) l'addition est associative et commutative, de neutre $\overline{0}$, et l'opposé de $\overline{a}$ est $\overline{-a}$;

ii) la multiplication est associative et commutative, de neutre $\overline{1}$;

iii) la multiplication est distributive par rapport à l'addition.

Démonstration. Ces identités résultent de celles de $\mathbb{Z}$ par passage aux classes. ■

Remarque 14

Pour $n \leq -2$, l'égalité $n\mathbb{Z}=|n|\mathbb{Z}$ permet de ramener le quotient à $\mathbb{Z}/|n|\mathbb{Z}$. Pour $n=\pm 1$, le quotient possède un seul élément. Pour $n=0$, $\mathbb{Z}/0\mathbb{Z}$ s'identifie à $\mathbb{Z}$.

Définition 3.3.2

Une classe $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible s'il existe $u \in \mathbb{Z}$ tel que

$$\overline{a}\,\overline{u}=\overline{1} \quad \Longleftrightarrow \quad au \equiv 1 \pmod{n}.$$

Exemple 13

Dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{3}\,\overline{2}=\overline{6}=\overline{1}$; ainsi $\overline{3}^{-1}=\overline{2}$. Comme $-2 \equiv 3 \pmod 5$, $\overline{-2}$ possède le même inverse.

Théorème 3.3.2 – Inversibilité modulo un entier

Pour $n \geq 2$ et $a \in \mathbb{Z}$,

$$\boxed{\overline{a} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z} \quad \Longleftrightarrow \quad \text{pgcd}(a,n)=1.}$$

Démonstration. Par Bézout,

$$\begin{aligned}\text{pgcd}(a,n)=1 &\Longleftrightarrow \exists u,v \in \mathbb{Z},\ au+nv=1\\ &\Longleftrightarrow \exists u \in \mathbb{Z},\ au \equiv 1 \pmod{n}.\end{aligned}$$

Dans ce cas, $\overline{u}$ est l'inverse de $\overline{a}$. ■

Corollaire 3.3.3

Pour un entier $p \geq 2$,

$$p \text{ est premier} \iff \mathbb{Z}/p\mathbb{Z} \text{ est un corps commutatif.}$$

Démonstration. Si p est premier, tout $a \in \{1, \ldots, p-1\}$ vérifie $\text{pgcd}(a, p) = 1$; toute classe non nulle est donc inversible. Réciproquement, si p est composé, écrivons $p = uv$ avec $1 < u, v < p$. Les classes $\overline{u}$ et $\overline{v}$ sont non nulles et leur produit est nul, ce qui est impossible dans un corps. ■

3.4 Notion de primalité dans $\mathbb{N}$ et dans $\mathbb{Z}$

3.4.1 Nombres premiers

Définition 3.4.1

Un entier naturel $p \geq 2$ est premier lorsque ses seuls diviseurs positifs sont 1 et p. En notant $\mathcal{D}_p = D_p \cap \mathbb{N}^*$,

$$p \text{ premier} \iff \mathcal{D}_p = \{1, p\}.$$

L'ensemble des nombres premiers positifs est noté $\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$.

Remarque 15 – Primalité dans $\mathbb{Z}$

Les unités de $\mathbb{Z}$ sont 1 et -1. Un entier $\pi \in \mathbb{Z} \setminus \{0, -1, 1\}$ est irréductible lorsque toute factorisation $\pi = ab$ impose $a = \pm 1$ ou $b = \pm 1$. Dans $\mathbb{Z}$, cela équivaut à $|\pi| \in \mathbb{P}$. Ses diviseurs sont alors $\{-|\pi|, -1, 1, |\pi|\}$. Les éléments premiers de $\mathbb{Z}$ sont donc les entiers $\pm p$, $p \in \mathbb{P}$; la propriété de divisibilité correspondante est établie par le théorème d'Euclide ci-dessous.

Lemme 3.4.1

Tout entier relatif a tel que $|a| \geq 2$ possède un diviseur premier positif.

Démonstration. L'ensemble $\{d \geq 2 : d \mid a\}$ est non vide car il contient $|a|$. Soit p son plus petit élément. Si p était composé, il admettrait un diviseur d tel que $1 < d < p$, et $d \mid a$, contradiction. ■

Théorème 3.4.1 – Infinité des nombres premiers

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

Démonstration. Supposons $\mathbb{P} = \{p_1, \ldots, p_k\}$. Le nombre $N = p_1 \cdots p_k + 1 \geq 2$ possède un diviseur premier p. Ce diviseur devrait être l'un des p_i, donc diviser à la fois $p_1 \cdots p_k$ et N, et par conséquent 1. C'est impossible. ■

3.4.2 Théorème fondamental de l'arithmétique

Théorème 3.4.2 – Décomposition en facteurs premiers

Tout entier $a \in \mathbb{Z}$ tel que $|a| \geq 2$ possède une unique écriture

$$\boxed{a = \varepsilon \prod_{i=1}^{r} p_i^{\alpha_i},}$$

où $\varepsilon \in \{-1, 1\}$, $p_1 < \cdots < p_r$ sont des nombres premiers positifs et $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$. Le signe est $\varepsilon = a/|a|$.

Lemme 3.4.2 – Récurrence forte

Soit $P(n)$ une propriété définie pour $n \geq n_0$. Si $P(n_0)$ est vraie et si, pour tout $n \geq n_0$,

$$\Big(P(n_0) \text{ et } \cdots \text{ et } P(n)\Big) \Longrightarrow P(n+1),$$

alors $P(n)$ est vraie pour tout $n \geq n_0$.

Démonstration de la décomposition. **Existence dans $\mathbb{N}$.** Le résultat est vrai pour 2. Supposons-le vrai pour tous les entiers compris entre 2 et n. Si $n+1$ est premier, sa décomposition est constituée d'un seul facteur. Sinon, $n+1 = bc$ avec $2 \leq b, c \leq n$. Les décompositions de b et c fournissent celle de $n+1$. La récurrence forte établit l'existence pour tout entier naturel au moins 2.

Unicité. Si $p, q \in \mathbb{P}$ sont distincts, alors $\operatorname{pgcd}(p, q) = 1$. Le théorème de Gauss implique qu'un nombre premier divisant un produit fini de nombres premiers est égal à l'un d'eux. Supposons

$$p_1 \cdots p_k = q_1 \cdots q_\ell$$

avec tous les facteurs premiers, répétitions autorisées. Le facteur p_1 est égal à l'un des q_j. Après permutation et simplification de ce facteur, on recommence. Les facteurs coïncident tous, avec les mêmes multiplicités ; sinon un produit non vide de nombres premiers serait égal à 1.

Extension à $\mathbb{Z}$. On applique le résultat à $|a|$ et on multiplie par $\varepsilon = a/|a|$. Le signe et la décomposition de la valeur absolue sont uniques. ■

Remarque 16

i) Pour $a = 1$ ou $a = -1$, on utilise le produit vide, égal à 1, et le signe $\varepsilon = a$.

ii) 0 ne possède pas de décomposition finie en facteurs premiers.

iii) Avec des facteurs premiers signés, l'unicité s'entend à l'ordre et à multiplication des facteurs par les unités ± 1 près.

Exemple 14

$$\begin{aligned} 8888 &= 2^3 \times 11 \times 101, \\ 1235 &= 5 \times 13 \times 19, \\ 5040 &= 2^4 \times 3^2 \times 5 \times 7, \\ -5040 &= -\Big(2^4 \times 3^2 \times 5 \times 7\Big). \end{aligned}$$

Proposition 3.4.1

Pour $p \in \mathbb{P}$ et $a \in \mathbb{Z}$,

$$\operatorname{pgcd}(p, a) = 1 \quad \Longleftrightarrow \quad p \nmid a.$$

Démonstration. Le PGCD est un diviseur positif de p, donc vaut 1 ou p. Il vaut p exactement lorsque $p \mid a$. ■

Théorème 3.4.3 – Théorème d'Euclide

Soient $p \in \mathbb{P}$ et $a, b \in \mathbb{Z}$. Alors

$$p \mid ab \quad \Longrightarrow \quad p \mid a \text{ ou } p \mid b.$$

La même propriété est vraie pour un élément premier signé $\pi = \pm p$. Si de plus $|a|$ et $|b|$ sont premiers, alors $p = |a|$ ou $p = |b|$.

Démonstration. Si $p \nmid a$, la proposition 3.4.1 donne $\operatorname{pgcd}(p, a) = 1$; le théorème 3.2.3 entraîne alors $p \mid b$. Pour $\pi = \pm p$, on utilise $\pi \mid c \Longleftrightarrow p \mid c$. Enfin, un diviseur premier positif de a premier à un signe près est nécessairement $|a|$, et de même pour b. ■

Lemme 3.4.3 – Intégrité de $\mathbb{Z}/p\mathbb{Z}$

Si $p \in \mathbb{P}$ et $a, b \in \mathbb{Z}$, alors

$$a \not\equiv 0 \pmod{p} \text{ et } b \not\equiv 0 \pmod{p} \quad \Longrightarrow \quad ab \not\equiv 0 \pmod{p}.$$

Démonstration. La contraposée est exactement le théorème d'Euclide : $p \mid ab \Longrightarrow p \mid a$ ou $p \mid b$. ■

Lemme 3.4.4

Pour $p \in \mathbb{P}$ et $x \in \mathbb{Z}$,

$$x^2 \equiv 1 \pmod{p} \quad \Longleftrightarrow \quad x \equiv 1 \pmod{p} \text{ ou } x \equiv -1 \pmod{p}.$$

Il y a deux classes solutions si $p > 2$, et une seule si $p = 2$.

Démonstration. On a $x^2 - 1 = (x-1)(x+1)$. Le théorème d'Euclide impose $p \mid x-1$ ou $p \mid x+1$. La réciproque est immédiate. Les classes de 1 et -1 sont égales exactement lorsque $p \mid 2$, c'est-à-dire $p = 2$. ■

Théorème 3.4.4 – Théorème de Wilson

Pour tout entier naturel $n \geq 2$,

$$\boxed{n \text{ est premier} \quad \Longleftrightarrow \quad (n-1)! \equiv -1 \pmod{n}.}$$

Démonstration. Si $n = p = 2$, on a $1! \equiv -1 \pmod 2$. Supposons $p > 2$ premier. Dans le corps $\mathbb{Z}/p\mathbb{Z}$, chaque classe non nulle possède un inverse. Les seules classes égales à leur inverse sont $\overline{1}$ et $\overline{-1}$. Les autres se regroupent par paires distinctes de produit $\overline{1}$. Ainsi

$$(p-1)! \equiv 1 \times (-1) \equiv -1 \pmod p.$$

Réciproquement, supposons $(n-1)! \equiv -1 \pmod n$ et n composé. Il existe d tel que $1 < d < n$ et $d \mid n$. Puisque d figure dans $(n-1)!$, on a $d \mid (n-1)!$. Mais la congruence modulo n donne aussi $d \mid (n-1)! + 1$. Donc $d \mid 1$, contradiction. ■

Corollaire 3.4.1 – Formulation pour un entier relatif

Pour $n \in \mathbb{Z}$ tel que $|n| \geq 2$,

$$|n| \text{ est premier} \iff (|n|-1)! \equiv -1 \pmod n.$$

Démonstration. On applique le théorème à $|n|$ et on utilise l'équivalence des congruences modulo n et modulo $|n|$. ■

3.5 Fonction indicatrice d'Euler

Définition 3.5.1

Pour $n \geq 2$, le groupe multiplicatif des unités de $\mathbb{Z}/n\mathbb{Z}$ est

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} : \text{pgcd}(a, n) = 1\}.$$

Ses éléments sont précisément les classes inversibles ; l'opération est la multiplication des classes et l'élément neutre est $\overline{1}$.

Définition 3.5.2

La fonction indicatrice d'Euler est la fonction $\phi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ définie par

$$\phi(n) = \text{Card}\{a \in \{1, \ldots, n\} : \text{pgcd}(a, n) = 1\}.$$

En particulier, $\phi(1) = 1$, et pour $n \geq 2$,

$$\phi(n) = \text{Card}(\mathbb{Z}/n\mathbb{Z})^\times.$$

Remarque 17

Pour un module relatif n tel que $|n| \geq 2$, le quotient $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/|n|\mathbb{Z}$ possède $\phi(|n|)$ classes inversibles. La fonction ϕ reste définie sur les entiers strictement positifs.

Propriété 3.5.1

Pour tout $p \in \mathbb{P}$, $\phi(p) = p - 1$. En particulier, $\phi(2) = 1$.

Démonstration. Les entiers $1, \ldots, p-1$ sont tous premiers avec p, tandis que $\text{pgcd}(p, p) = p$. ■

Exemple 15

$$(\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}, \qquad \phi(12) = 4.$$

Le quotient $\mathbb{Z}/(-12)\mathbb{Z}$ possède les mêmes classes et les mêmes unités.

Références bibliographiques

[1] Jean-Marie De Koninck et Armel Mercier, *1001 Problems in Classical Number Theory*, American Mathematical Society, 2007.

[2] François de Marçay, *Arithmétique dans $\mathbb{Z}$ et dans $\mathbb{Z}/n\mathbb{Z}$*, Département de Mathématiques d'Orsay, Université Paris-Saclay, France.

[3] Abdallah Hammam, *Arithmétique des Entiers*, Université Moulay Ismaïl, Faculté des sciences, Département de Mathématiques.