

Arithmétique élémentaire

B. Seddoug. Médiane Sup, Oujda.

I Numération

I.1 Définition - Exemples

Théorème I.1 Soit $q \in \mathbb{N}, q \geq 2$. Pour tout entier $N \in \mathbb{N}$, il existe une unique suite $(s_n)_{n \in \mathbb{N}}$ nulle à partir d'un certain rang telle que

$$N = s_0 + s_1q + \dots + s_nq^n \text{ avec } n = \max \{k \in \mathbb{N} \mid s_k \neq 0\} \quad (I.1)$$

Définition 1 Si N vérifie (I.1), on écrit

$$N = \overline{s_n s_{n-1} \dots s_0}^q \quad (I.2)$$

L'écriture (I.2) est appelé la représentation de N en base q (ou dans le système à base q).

Preuve du théorème I.1: L'existence se fait par récurrence transfinie. L'unicité se fait par absurde. •

Exemple 1 $1 = \overline{1}^q; 2 = \overline{2}^q; \dots; q-1 = \overline{q-1}^q$ et $q = \overline{10}^q; q+1 = \overline{11}^q$.

I.2 Numération décimale

Dans le cas $q = 10$, le système de numération est dit décimale. Les symboles utilisés sont

$$0; 1; 2; 3; 4; 5; 6; 7; 8 \text{ et } 9.$$

Remarque 1 Dans ce cas on écrit sans la barre dessus.

Application à la divisibilité dans \mathbb{N}

- Divisibilité par 2 et 5: On a $10 = 2 \times 5$, donc

$$N = \overline{s_n s_{n-1} \dots s_0} \text{ est divisible par } 2 \iff s_0 \in \{0; 2; 4; 6; 8\}.$$

$$N = \overline{s_n s_{n-1} \dots s_0} \text{ est divisible par } 5 \iff s_0 \in \{0; 5\}.$$

- Divisibilité par 3 et 9: On a $10 = 1 + 3 \times 3, 100 = 1 + 3 \times 3 \times 11 \dots$ donc

$$N = \overline{s_n s_{n-1} \dots s_0} \text{ est divisible par } 3 \iff \sum_{k=0}^n s_k \text{ est divisible par } 3.$$

$$N = \overline{s_n s_{n-1} \dots s_0} \text{ est divisible par } 9 \iff \sum_{k=0}^n s_k \text{ est divisible par } 9.$$

- Divisibilité par 4: On a $100 = 4 \times 25, 1000 = 4 \times 250 \dots$ donc

$$N = \overline{s_n s_{n-1} \dots s_0} \text{ est divisible par } 4 \iff s_1 s_0 \text{ est divisible par } 4.$$

I.3 Numération binaire

Dans le cas où $q = 2$, le système de numération est dit binaire. Les symboles utilisés sont

0 et 1.

Exemple 2 Voir S.I : $2 = \overline{10}^2; 3 = \overline{11}^2$.

Exercice 1 Dans quelle base le nombre 880 s'écrit-il 12010?

II Arithmétique dans l'anneau \mathbb{Z}

II.1 La congruence

Définition 2 Deux entiers a et b sont dit congrus modulo n ($n \in \mathbb{N}$) si $a - b \in n\mathbb{Z}$. On note alors $a \equiv b [n]$ ou $a \equiv b \pmod{n}$. On a donc

$$a \equiv b [n] \iff a - b \in n\mathbb{Z} \iff \exists k \in \mathbb{Z} \mid a = nk + b.$$

Propriétés

P II.1 La relation de congruence modulo n est une relation d'équivalence sur \mathbb{Z} .

P II.2 $\forall a, b, a', b' \in \mathbb{Z}$ et $\forall n \in \mathbb{N}$, on a

$$\left. \begin{array}{l} a \equiv b [n] \\ a' \equiv b' [n] \end{array} \right\} \implies a + a' \equiv b + b' [n] \text{ et } a \times a' \equiv b \times b' [n].$$

Cette propriété est appelée la compatibilité de la congruence modulo n avec les opérations $+$ et \times dans \mathbb{Z} . Elle permet de définir sur l'ensemble quotient $\mathbb{Z}/\equiv [n]$ des opérations en posant

$$\bar{a} + \bar{b} = \overline{a + b} \text{ et } \bar{a} \times \bar{b} = \overline{a \times b}. \quad (II.1)$$

P II.3 L'ensemble quotient modulo n est noté $\mathbb{Z}/n\mathbb{Z}$, il est de cardinal n en plus

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}; \dots; \overline{n-1}\} \text{ en bijection avec } \llbracket 0, n-1 \rrbracket.$$

II.2 Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

Théorème II.1 Les opérations définies sur $\mathbb{Z}/n\mathbb{Z}$ par les relations (II.1) munissent $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau commutatif.

De plus l'application $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}; a \longmapsto \bar{a}$ est un morphisme surjectif d'anneaux.

Remarque 2 L'anneau $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n et sa structure sous jacente de groupe est cyclique. $\bar{0}$

Exemple 3 Tables d'anneaux de $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$:

+	0	1
0	0	1
1	1	0

\times	0	1
0	0	0
1	0	1

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

\times	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Remarque 3 On remarque que $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ sont des corps, alors que $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre.

Exercice 2 Résoudre dans $\mathbb{Z}/6\mathbb{Z}$ les équations:

$$X^5 - 1 = 0 \quad ; \quad X^5 - 2 = 0 \quad ; \quad X^4 + X^3 + 2 = 0.$$

II.3 PGCD et PPCM

II.3.1 Définitions - Exemples

Définition 3 (PGCD) Soient $a, b \in \mathbb{Z}$, on appelle Plus Grand Diviseur Commun de a et b l'unique entier naturel d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On note $d = \text{pgcd}(a, b)$ ou $d = a \wedge b$. On a donc

$$d = \text{pgcd}(a, b) \iff a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

Remarque 4 $a\mathbb{Z} + b\mathbb{Z}$ étant un sous groupe de \mathbb{Z} il est donc de la forme $d\mathbb{Z}$ où $d = \min[(a\mathbb{Z} + b\mathbb{Z}) \cap]$

Proposition 1 (Caractérisation du PGCD) Soient $a, b \in \mathbb{Z}$, et $d \in \mathbb{N}$. Les propriétés suivantes sont équivalentes:

- (i) $d = \text{pgcd}(a, b)$.
- (ii) d est un diviseur commun à a et b , et tout diviseur commun à a et b divise d .
- (iii) d est un diviseur commun à a et b , et tout diviseur commun à a et b est $\leq d$.

Preuve: (i) \implies (ii) et (i) \implies (iii): évident d'après la définition.

(ii) \implies (i): On pose $d' = \text{pgcd}(a, b)$ et on montre que $d' = d$.

Exemple 4 $0 \wedge n = n, \forall n \in \mathbb{Z}; 3 \wedge 2 = 1; 12 \wedge 8 = 4...$

Définition 4 (Entiers premiers entre eux) Si $\text{pgcd}(a, b) = 1$, on dit que a et b sont premiers entre eux. i.e:

$$a \text{ et } b \text{ premier entre eux si et seulement si } a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}.$$

Exemple 5 2 est premier avec tout entier impair.

Définition 5 (PPCM) Soient $a, b \in \mathbb{Z}$, on appelle Plus Petit Multiple Commun de a et b l'unique entier naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. On note $m = \text{ppcm}(a, b)$ ou $d = a \vee b$. On a donc

$$m = \text{ppcm}(a, b) \iff a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}.$$

Remarque 5 $a\mathbb{Z} \cap b\mathbb{Z}$ étant un sous groupe de \mathbb{Z} il est donc de la forme $m\mathbb{Z}$ où $m = \min[(a\mathbb{Z} \cap b\mathbb{Z}) \cap]$

Proposition 2 (Caractérisation du PPCM) Soient $a, b \in \mathbb{Z}$, et $m \in \mathbb{N}$. Les propriétés suivantes sont équivalentes:

- (i) $m = \text{ppcm}(a, b)$.
- (ii) m est un multiple commun à a et b , et tout multiple commun à a et b est multiple de m .
- (iii) m est un multiple commun à a et b , et tout multiple commun à a et b est $\geq m$.

Preuve: (i) \implies (ii) et (i) \implies (iii): évident d'après la définition.

(ii) \implies (i): On pose $m' = \text{ppcm}(a, b)$ et on montre que $m' = m$.

Exemple 6 $3 \vee 2 = 6; 12 \vee 8 = 24...$

Définition 6 (PPCM et PGCD d'une famille d'entiers) En général si a_1, a_2, \dots, a_n sont des entiers, on définit leur PGCD et PPCM par:

- $\text{pgcd}(a_1, a_2, \dots, a_n) = d$ si et seulement si $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$.
- $\text{ppcm}(a_1, a_2, \dots, a_n) = m$ si et seulement si $a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = m\mathbb{Z}$.

De même on dit que a_1, a_2, \dots, a_n sont premiers entre eux (dans leur ensemble) si

$$\text{pgcd}(a_1, a_2, \dots, a_n) = 1.$$

II.3.2 Propriétés

Soient a, b et c des entiers relatifs.

P II.4 $\text{pgcd}(ab, ac) = |a| \text{pgcd}(b, c)$.

En particulier si $d = \text{pgcd}(b, c)$ alors $\frac{b}{d} \wedge \frac{c}{d} = 1$.

P II.5 $\text{ppcm}(ab, ac) = |a| \text{ppcm}(b, c)$.

P II.6 Si $a = bq + r$ alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

II.3.3 Algorithme d'Euclide

On suppose $a, b \in \mathbb{N}$. L'algorithme d'Euclide est basé sur la propriété (PII.6) ci-dessus. Donc il consiste à faire des D.E successives jusqu'à avoir un reste nul.

Algorithme

1. Lecture de a et b ;
2. Tant que $b \neq 0$ Faire
3. Division Euclidienne de a par b : $a = bq + r$;
4. $a \leftarrow b; b \leftarrow r$;
5. Fin Faire
6. Résultat $\text{pgcd}(a, b) = a$ (le dernier reste non nul).

Remarque 6 La suites des restes r dans les Divisions Euclidiennes est strictement décroissantes, donc s'arrête à un certain rang, d'où la convergence de l'algorithme.

Exemple 7 Exécuter l'algorithme avec $a = 136$ et $b = 18$.

II.4 Théorème de Bezout et conséquence

Théorème II.2 (de Bezout) Soient $a, b \in \mathbb{Z}$, alors a et b sont premiers entre eux si et seulement s'il existe $(u, v) \in \mathbb{Z}^2$ tels que

$$au + bv = 1 \tag{II.2}$$

Définition 7 Un couple (u, v) vérifiant (II.2) est appelé un couple de coefficients de Bezout.

Remarque 7 Le théorème sans difficulté à une famille d'entiers:

$$\text{pgcd}(a_1, a_2, \dots, a_n) = 1 \iff \exists (u_1, \dots, u_n) \in \mathbb{Z}^n \mid \sum_{i=1}^n a_i u_i = 1.$$

Démonstration du théorème de Bezout: \implies Si $a \wedge b = 1$ alors $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ donc u et v existent.

\impliedby Si $\exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$ alors $1 \in a\mathbb{Z} + b\mathbb{Z}$ donc $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$. .

Proposition 3 Si $a \wedge b = 1$ alors il existe une infinité de couples de coefficients de Bezout.

En effet: Si (u_0, v_0) vérifient $au_0 + bv_0 = 1$ alors $\forall m \in \mathbb{Z} : (u = u_0 + mb, v = v_0 - ma)$ répond à la question. .

Exemple de détermination d'un couple de coefficients de Bezout

La méthode des divisions successives avec $a = 132, b = 35$, on a successivement:

$$\begin{array}{ll} 132 = 35 \times 3 + 27 & 132 \wedge 35 = 35 \wedge 27 \\ 35 = 27 \times 1 + 8 & 35 \wedge 27 = 27 \wedge 8 \\ 27 = 8 \times 3 + 3 & 27 \wedge 8 = 8 \wedge 3 \\ 8 = 3 \times 2 + 2 & 8 \wedge 3 = 3 \wedge 2 \\ 3 = 2 \times 1 + 1 & 3 \wedge 2 = 2 \wedge 1 = 1 \end{array}$$

Remontée:

$$\begin{aligned} 1 &= 3 - 2 \times 1 \\ &= 3 - (8 - 3 \times 2) \times 1 = 3 + 8 + 3 \times 2 \\ &= 3 \times 3 - 8 = 3 \times (27 - 3 \times 8) - 8 = -9 \times 8 - 8 + 3 \times 27 \\ &= -10 \times 8 + 3 \times 27 \\ &= -10 \times (35 - 27) + 3 \times 27 = 10 \times 27 + 3 \times 27 - 10 \times 35 \\ &= 13 \times 27 - 10 \times 35 \\ &= 13 \times (132 - 35 \times 3) - 10 \times 35 = 13 \times 132 - (13 \times 3 + 10) \times 35 \\ &= 13 \times 132 - 49 \times 35. \end{aligned}$$

Donc $u = 13$ et $v = -49$ répondent à la question.

Théorème II.3 (de Gauss) Soient $a, b, c \in \mathbb{Z}$. On a

$$\left. \begin{array}{l} a \text{ divise } bc \\ \text{et} \\ a \wedge b = 1 \end{array} \right\} \implies a \text{ divise } c.$$

Preuve: $a \wedge b = 1$ donc il existe (u, v) tel que $au + bv = 1$ et par suite $acu + bcv = c$.

Et comme a divise bc alors il existe a' tel que $bc = aa'$.

Donc $acu + aa'v = c$ c'est à dire $a(cu + a'v) = c$.

Donc c divise a . .

Théorème II.4 Soient a, b_1, b_2, \dots, b_n des entiers

Si $a \wedge b_i = 1$ pour tout $i \in \llbracket 1, n \rrbracket$ alors $a \wedge \prod_{i=1}^n b_i = 1$.

Preuve: Bezout et une récurrence. .

Théorème II.5 Soient a, b deux entiers tels que $a \wedge b = 1$ alors $a \vee b = ab$.

En général si b_1, b_2, \dots, b_n sont des entiers deux à deux premiers entre eux alors

$$\text{ppcm}(b_1, \dots, b_n) = \prod_{i=1}^n b_i.$$

Remarque 8 On a aussi la réciproque $a \vee b = ab \implies a \wedge b = 1$.

En effet: Si on suppose $a \wedge b = d > 1$ alors

$$\text{ppcm}(a, b) = d \times \text{ppcm}\left(\frac{a}{d}, \frac{b}{d}\right) = d \times \frac{a}{d} \times \frac{b}{d} = \frac{ab}{d} \neq d$$

Ce qui absurde. .

Démonstration du théorème II.5: Posons $m = a \vee b$,

Il existe a', b' tels que $m = aa' = bb'$, donc a divise bb' .

Comme $a \wedge b = 1$ alors a divise b' et par suite il existe b'' tel que $b' = ab''$.

Donc $m = bab''$ c'est à dire ab divise m et comme m divise ab alors $m = ab$. .

Théorème II.6 Soient a, b deux entiers et $d \in \mathbb{N}$, on a l'équivalence

$$a \wedge b = d \iff \frac{a}{d} \wedge \frac{b}{d} = 1.$$

Théorème II.7 (Calcul du PPCM) Pour tout $(a, b) \in \mathbb{Z}^2$, on a

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

Exercice 3 Déterminer tout les couples $(u, v) \in \mathbb{Z}^2$ tels que

$$323u - 391v = 612. \tag{II.3}$$

Réponse: On a $323 \wedge 391 = 323 \wedge 68 = 68 \wedge 51 = 51 \wedge 17 = 17$ car $51 = 3 \times 17$.

Donc

$$\begin{aligned} 323u - 391v &= 612 \iff \frac{323}{17}u - \frac{391}{17}v = \frac{612}{17} \\ &\iff 19u - 23v = 36 \end{aligned}$$

Comme $19 \wedge 23 = 1$ alors si (u_0, v_0) est un couple de coefficients de Bezout alors $(36u_0, 36v_0)$ est une solution particulière de (II.3).

Donc les solutions sont de la forme $(u = 36u_0 + 23k, v = 36v_0 + 19k)$. .

Forme irréductible d'un rationnel

Proposition 4 Pour tout rationnel $r \in \mathbb{Q}^*$, il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que

$$r = \frac{p}{q} \text{ et } p \wedge q = 1.$$

Le couple (p, q) est alors appelé représentant irréductible de r .

Preuve: Si $r = \frac{a}{b}$ tel que $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ et $d = a \wedge b$, alors $p = \frac{a}{d}$ et $q = \frac{b}{d}$ répondent à la question d'existence.

Pour l'unicité, si $\frac{p}{q} = \frac{p'}{q'}$ avec $p \wedge q = p' \wedge q' = 1$ alors $pq' = p'q$.

Donc p divise $p'q$ et comme $p \wedge q = 1$ alors p divise p' , de même p' divise p par un même raisonnement.

Enfin $p = p'$ et $q = q'$, d'où l'unicité. .

Générateurs d'un groupe cyclique

Proposition 5 Soit $G = \{e; a; a^2; \dots; a^{n-1}\}$ un groupe cyclique de cardinal n . Alors a^k est un générateur de G si et seulement si $k \wedge n = 1$.

Preuve: \implies Si a^k est un générateur de G alors $\exists p \in \mathbb{Z}$ tel que $(a^k)^p = a$, c'est à dire $a^{kp-1} = e$ donc $\exists q \in \mathbb{Z}$ tel que $kp-1 = nq$ donc $k \wedge n = 1$.

\impliedby si $k \wedge n = 1$ alors $\exists u, v \in \mathbb{Z}$ tels que $ku + vn = 1$ ou $ku - 1 = -vn$,

donc $a^{ku-1} = (a^n)^{-v} = e$, c'est à dire $(a^k)^u = a$, donc a^k est générateur de G . .

Inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition 6 Soit $n \in \mathbb{N}^*$, Pour tout $a \in \mathbb{Z}$, on a

\bar{a} inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$.

En particulier: $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Preuve: La même que celle de la proposition 5. .

Ordre de produit d'élément d'un groupe

Proposition 7 Soient G un groupe, a et b deux éléments de G d'ordre respectifs n et m .

Si $ab = ba$ et $gr(a) \cap gr(b) = \{e\}$ alors $ord(ab) = ppcm(m, n)$.

En particulier: si $m \wedge n = 1$ et $ab = ba$ alors $ord(ab) = mn$.

Preuve: Soit $\mu = m \vee n$, on a $(ab)^\mu = a^\mu b^\mu = e$.

Réciproquement, si $(ab)^k = e$, alors $a^k = b^{-k} \in gr(a) \cap gr(b)$, donc $a^k = b^k = e$.

Donc m et n divisent k donc μ divise k .

En particulier si $m \wedge n = 1$ alors $gr(a) \cap gr(b) = \{e\}$, car si non, il existent u, v dans \mathbb{Z} tels que $a^u = b^v \neq e$. .

III Nombres premiers**III.1 Définitions - Exemples**

Définition 8 On appelle nombre premier tout entier naturel $p \geq 2$ dont les seuls diviseurs dans \mathbb{N} sont 1 et p .

Exemple 8 Les entiers 2; 3; 5; 7; 11; 13 sont premiers.

Les nombres de Fermat: $F_n = 2^{2^n} + 1$ sont premiers pour $n = 0, 1, 2, 3, 4$ mais pour $n = 5$.

Théorème III.1 Soit p un nombre premier.

1. p est premier avec tout entier qu'il ne divise pas:

$$\forall k \in \mathbb{Z} : p \wedge k = 1 \iff p \text{ ne divise pas } k.$$

2. En particulier deux entiers premiers distincts sont premiers entre eux.

Exercice 4 Si p premier alors p divise \mathbb{C}_p^k pour tout k tel que $1 \leq k \leq p-1$.

III.2 Décomposition d'un entier en facteurs premiers

Théorème III.2 Tout entier $N \geq 2$ admet au moins un diviseur premier.

Preuve: p = plus petit élément de l'ensemble des diviseurs de N , i.e:

$$p = \min \{q \in \mathbb{N}^* \setminus \{1\} \mid q \text{ divise } N\}$$

est un entier premier, si non il est composée: $p = p_1 p_2$ avec $2 \leq p_i \leq p-1$ ce qui est absurde. .

Corollaire III.3 (Euclide) L'ensemble \mathcal{P} des nombres premiers est infini.

Preuve: Si \mathcal{P} est fini alors il est majoré par un $N \geq 2$. L'entier $N! + 1$ admet un diviseur premier différent de tous les entier de l'intervalle $\llbracket 1, N \rrbracket$, ce qui est absurde. .

Théorème III.4 (Décomposition en facteurs premiers) Soit N un entier $N \geq 2$. On note p_1, p_2, \dots, p_n tous les diviseurs premiers de N .

Il existe un unique n -uplet $(\alpha_1, \alpha_2, \dots, \alpha_n) \in (\mathbb{N}^*)^n$ tel que

$$N = \prod_{i=1}^n p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}.$$

Preuve: Pour chaque $i \in \llbracket 1, n \rrbracket$, on pose $\alpha_i = \max \{\alpha \in \mathbb{N} \mid p_i^\alpha \text{ divise } N\}$. .

Théorème III.5 (Calcul du PGCD et PPCM) Soient $a = \prod_{i=1}^n p_i^{\alpha_i}$ et $b = \prod_{i=1}^n p_i^{\beta_i}$.

$$a \wedge b = \prod_{i=1}^n p_i^{\min\{\alpha_i; \beta_i\}} \text{ et } a \vee b = \prod_{i=1}^n p_i^{\max\{\alpha_i; \beta_i\}}.$$