Chapitre C3

Arithmétique

Objectifs

- Diviseurs et multiples.
- Division euclidienne.
- PGCD, PPCM.
- Théorèmes d'arithmétique.
- Nombres premiers.

1 Outils de l'arithmétique

1.1 Divisibilité

Définition C3.1

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

$$\exists k \in \mathbb{Z},\ b = ak.$$

On note alors $a \mid b$ et on dit que b est **divisible** par a, ou que b est **un multiple** de a.

Notation. Soit $a \in \mathbb{Z}$. On note $a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$ l'ensemble des multiples de a.

Proposition C3.2

(i) La relation de divisibilité est une relation réflexive et transitive sur $\mathbb{Z}$.

(ii) $\forall a, b \in \mathbb{Z}$, $(a \mid b \text{ et } b \mid a) \Leftrightarrow a = \pm b$.

Soit $a, b \in \mathbb{Z}$. On dit que a et b sont **associés** lorsqu'il existe $u \in \mathbb{Z}^\times$ tel que $a = ub$.

Notation. On note $a \sim b \Leftrightarrow a = \pm b$.

Proposition C3.3

Soit $a, b, c, d \in \mathbb{Z}$.

(i) Si $a \mid b$ et $a \mid c$, alors $\forall \lambda, \mu \in \mathbb{Z}$, $a \mid (\lambda b + \mu c)$.

(ii) Si $a \mid b$ et $c \mid d$, alors $ac \mid bd$ et $\forall k \in \mathbb{N}$, $a^k \mid b^k$

(iii) Si $ab \mid ac$ et $a \neq 0$, alors $b \mid c$.

1.2 Congruences

Définition C3.4

Soit $a, b, n \in \mathbb{Z}$. On dit que a est **congru à** b **modulo** n et on note $a \equiv b[n]$ lorsque n divise $a - b$. Autrement dit

$$a \equiv b\ [n] \Leftrightarrow \exists k \in \mathbb{Z},\ a = b + kn.$$

Notation. On note aussi $a \equiv b \mod n$ ou $a \equiv b \pmod{n}$.

Remarque. Soit $d, n \in \mathbb{Z}$. On a

$$d \mid n \Leftrightarrow n \equiv 0\ [d].$$

Proposition C3.5

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

Proposition C3.6

Soit $a, a', b, b', m, n \in \mathbb{Z}$ et soit $k \in \mathbb{N}$.

(i) Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, alors $a + a' \equiv b + b'\ [n]$.

(ii) $a \equiv b\ [n] \Rightarrow ma \equiv mb\ [n]$.

(iii) Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, alors $aa' \equiv bb'\ [n]$ et $a^k \equiv b^k\ [n]$.

1.3 Division euclidienne

Théorème et définition C3.7

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

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

On dit que q est le **quotient** et r le **reste** de la **division euclidienne** de a par b.

Proposition C3.8

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

2 PGCD, PPCM

2.1 Définition

Proposition et définition C3.9

Soit $a, b \in \mathbb{Z}$. Si $a = b = 0$, on note conventionnellement $a \wedge b = 0$. Sinon, l'ensemble des diviseurs communs à a et b possède un plus grand élément (pour la relation d'ordre $\leqslant$), noté $a \wedge b$.
L'entier $a \wedge b$ est appelé **plus grand commun diviseur** (**PGCD**) de a et b.

Proposition et définition C3.10

Soit $a, b \in \mathbb{Z}$. Si $a = 0$ ou $b = 0$, on note conventionnellement $a \vee b = 0$. Sinon, l'ensemble des multiples strictement positifs communs à a et b possède un plus petit élément (pour la relation d'ordre $\leqslant$), noté $a \vee b$.
L'entier $a \vee b$ est appelé **plus petit commun multiple** (**PPCM**) de a et b.

Proposition C3.11

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

(i) $a \wedge b \in \mathbb{N}$,
(ii) $(a \wedge b) \mid a$ et $(a \wedge b) \mid b$,
(iii) $a \wedge b = b \wedge a$,
(iv) $a \wedge 0 = |a|$,
(v) $a \vee b \in \mathbb{N}$,
(vi) $a \mid (a \vee b)$ et $b \mid (a \vee b)$,
(vii) $a \vee b = b \vee a$,
(viii) si $a \neq 0$, alors $a \vee 1 = |a|$.

2.2 Euclide, Bézout et Gauß

Théorème C3.12

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Soit r le reste de la division euclidienne de a par b. Alors

$$a \wedge b = r \wedge b.$$

Proposition C3.13 (Algorithme d'Euclide)

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.
On pose $r_0 = |a|$, $r_1 = |b|$ puis pour tout $n \in \mathbb{N}$ tel que $r_n \neq 0$, r_{n+1} le reste de la division euclidienne de r_{n-1} par r_n.
Il existe un plus petit $N \in \mathbb{N}^*$ tel que $r_N = 0$. Dans ce cas $r_{N-1} = a \wedge b$.

Théorème et définition C3.14 (Relation de Bézout)

Soit $(a, b) \in \mathbb{Z}^2$. Il existe $(u, v) \in \mathbb{Z}^2$ tels que

$$au + bv = a \wedge b.$$

Les entiers u et v sont appelés **coefficients de Bézout** de a et b.

Remarque. On peut étendre l'algorithme d'Euclide ci-dessus pour déterminer les nombres u et v. Avec les notations précédentes, posons également, pour tout $1 \leqslant n < N$, q_n le quotient dans la division euclidienne

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

On définit deux familles d'entiers $(\lambda_n)_{0 \leqslant n \leqslant N}$ et $(\mu_n)_{0 \leqslant n \leqslant N}$ par $(\lambda_0, \mu_0) = (1, 0)$, $(\lambda_1, \mu_1) = (0, 1)$ et

$$\forall 0 < n < N, \begin{cases} \lambda_{n+1} = \lambda_{n-1} - q_n \lambda_n \\ \mu_{n+1} = \mu_{n-1} - q_n \mu_n \end{cases} .$$

On a alors pour tout $n \in [\![0, N]\!]$: $\lambda_n a + \mu_n b = r_n$.
Comme $r_{N-1} = a \wedge b$, $(u, v) = (\lambda_{N-1}, \mu_{N-1})$ est un couple de coefficients de Bézout de a et b.
De plus, comme $r_N = 0$, on a $\lambda_N a + \mu_N b = 0$. Et alors $|\lambda_N a| = |\mu_N b| = a \vee b$.

Proposition C3.15

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

(i)
- $\forall d \in \mathbb{Z}$, $d \mid a$ et $d \mid b \Leftrightarrow d \mid (a \wedge b)$.
- Les diviseurs communs à a et b sont les diviseurs de $a \wedge b$.
- $a \wedge b$ est le plus grand commun diviseur de a et b au sens de la divisibilité.

(ii)
- $\forall m \in \mathbb{Z}$, $a \mid m$ et $b \mid m \Leftrightarrow (a \vee b) \mid m$.
- Les multiples communs à a et b sont les multiples de $a \vee b$.
- $a \vee b$ est le plus petit commun multiple de a et b au sens de la divisibilité.

Proposition C3.16

Soit $a, b \in \mathbb{Z}$ et $k \in \mathbb{N}$.

(i) $(ka) \wedge (kb) = k(a \wedge b)$,

(ii) $(ka) \vee (kb) = k(a \vee b)$.

Proposition C3.17

Soit $a, b \in \mathbb{Z}$ et $d = a \wedge b$. Il existe a', b' tels que

$$a = da',\ b = db' \text{ et } a' \wedge b' = 1.$$

Définition C3.18

Soit $a, b \in \mathbb{Z}$. On dit que a et b sont **premiers entre eux** lorsque $a \wedge b = 1$.

Remarque. La propriété précédente permet de définir la forme irréductible d'un nombre rationnel.

Théorème C3.19 (Bézout)

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

$$a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2,\ au + bv = 1.$$

Corollaire C3.20

Soit $a, b, c \in \mathbb{Z}$.

(i) Si $a \wedge b = 1$ et $c \mid b$, alors $a \wedge c = 1$.

(ii) Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge (bc) = 1$.

(iii) Pour tout $k \in \mathbb{N}$, $a^k \wedge b^k = (a \wedge b)^k$.

Théorème C3.21 (Gauß)

Soit $a, b, c \in \mathbb{Z}$. Si $a \mid (bc)$ et $a \wedge b = 1$, alors $a \mid c$.

Corollaire C3.22

Soit $a, b, m, n \in \mathbb{Z}$.

(i) Si $am \equiv bm\ [n]$ et $m \wedge n = 1$, alors $a \equiv b\ [n]$.

(ii) Si $a \mid n$, $b \mid n$ et $a \wedge b = 1$, alors $(ab) \mid n$.

Théorème C3.23

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

(i) Si $a \wedge b = 1$, alors $a \vee b = |ab|$.

(ii) $(a \wedge b)(a \vee b) = |ab|$.

2.3 Cas d'une famille de nombres entiers

Proposition C3.24

$\wedge$ et $\vee$ sont des lois de composition internes commutatives et associatives sur $\mathbb{Z}$.

Définition C3.25

Soit $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n \in \mathbb{Z}$. On appelle **plus grand commun diviseur** (resp. **plus petit commun multiple**) de $a_1, \ldots, a_n$ le nombre $a_1 \wedge \ldots \wedge a_n$ (resp. $a_1 \vee \ldots \vee a_n$).

Remarque. Cette définition ne dépend ni de l'ordre des nombres a_i ni de la manière de parenthéser l'expression.

Notation. On note $\displaystyle\bigwedge_{i=1}^{n} a_i$ (resp. $\displaystyle\bigvee_{i=1}^{n} a_i$) avec la convention d'un PGCD nul et d'un PPCM égal à 1 si $n = 0$.

Théorème C3.26

Soit $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n \in \mathbb{Z}$.

(i) Soit $d \in \mathbb{Z}$. $(\forall i \in [\![1, n]\!],\ d \mid a_i) \Leftrightarrow d \mid \left(\displaystyle\bigwedge_{i=1}^{n} a_i\right)$.

(ii) Soit $m \in \mathbb{Z}$. $(\forall i \in [\![1, n]\!],\ a_i \mid m) \Leftrightarrow \left(\displaystyle\bigvee_{i=1}^{n} a_i\right) \mid m$.

Remarques. Par convention, si tous les a_i sont nuls, alors leur PGCD est 0 ; et si l'un des a_i est nul, alors leur PPCM est 0.
Sinon, à nouveau, les termes « plus grand » et « plus petit » dans PGCD et PPCM valent au sens de la relation de divisibilité ainsi qu'au sens de la relation d'ordre usuelle, pour les diviseurs et multiples positifs.

Définition C3.27

Soit $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n \in \mathbb{Z}$.

(i) On dit que $a_1, \ldots, a_n$ sont **premiers entre eux dans leur ensemble** lorsque $\displaystyle\bigwedge_{i=1}^{n} a_i = 1$.

(ii) On dit que $a_1, \ldots, a_n$ sont **premiers entre eux deux à deux** lorsque

$$\forall i, j \in [\![1, n]\!],\ (i \neq j \Rightarrow a_i \wedge a_j = 1).$$

Proposition C3.28

Des entiers premiers entre eux deux à deux sont premiers entre eux dans leur ensemble.

Théorème C3.29 (Bézout)

Soit $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{Z}$.

(i) $\exists u_1, \dots, u_n \in \mathbb{Z}, \ \sum_{i=1}^{n} u_i a_i = \bigwedge_{i=1}^{n} a_i$.

(ii) $\bigwedge_{i=1}^{n} a_i = 1 \Leftrightarrow \exists u_1, \dots, u_n \in \mathbb{Z}, \ \sum_{i=1}^{n} u_i a_i = 1$.

Théorème C3.30

Soit $n \in \mathbb{N}$ et $a_1, \dots, a_n \in \mathbb{Z}$ premiers entre eux dans leur ensemble. Alors

$$\bigvee_{i=1}^{n} a_i = \left| \prod_{i=1}^{n} a_i \right|.$$

3 Nombres premiers

3.1 Définition

Définition C3.31

Un **nombre premier** est un nombre entier $p \geqslant 2$ dont les seuls diviseurs positifs sont 1 et p.

Notation. On note $\mathbb{P}$ l'ensemble des nombres premiers.

Proposition C3.32

(i) Soit $p \in \mathbb{P}$ et $a \in \mathbb{Z}$. On a $p \mid a$ ou $p \wedge a = 1$.

(ii) Deux nombres premiers sont soit égaux soit premiers entre eux.

(iii) Soit $p \in \mathbb{P}$ et $a, b \in \mathbb{Z}$. Si $p \mid (ab)$, alors $p \mid a$ ou $p \mid b$.

Théorème C3.33

Il existe une infinité de nombres premiers.

Lemme C3.34

Soit $p \in \mathbb{P}$ et $k \in [\![0, p-1]\!]$. On a $p \mid \binom{p}{k}$.

Théorème C3.35 (Petit théorème de Fermat)

Soit $p \in \mathbb{P}$.

(i) $\forall n \in \mathbb{Z}$, $n^p \equiv n\ [p]$,

(ii) $\forall n \in \mathbb{Z}$, $(n \wedge p = 1 \Rightarrow n^{p-1} \equiv 1\ [p])$.

3.2 Valuations p-adiques

Proposition et définition C3.36

Soit $p \in \mathbb{P}$ et $n \in \mathbb{Z} \setminus \{0\}$. L'ensemble $\left\{k \in \mathbb{N} \mid p^k \text{ divise } n\right\}$ admet un plus grand élément, appelé **valuation p-adique** de n et noté $v_p(n)$.

Remarque. Par convention, $v_p(0) = +\infty$. Par ailleurs $v_p(n) = 0$ si et seulement si p ne divise pas n.

Proposition C3.37

Soit $n \in \mathbb{Z}$, $p \in \mathbb{P}$ et $k \in \mathbb{N}$.

(i) $v_p(n) \geqslant k \Leftrightarrow p^k \mid n \Leftrightarrow \exists m \in \mathbb{Z},\ n = p^k m$.

(ii) $v_p(n) = k \Leftrightarrow (p^k \mid n \text{ et } p^{k+1} \nmid n) \Leftrightarrow \exists m \in \mathbb{Z},\ (n = p^k m \text{ et } p \wedge m = 1)$.

Proposition C3.38

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

(i) Si $a \mid b$, alors $v_p(a) \leqslant v_p(b)$,

(ii) $v_p(ab) = v_p(a) + v_p(b)$,

(iii) $v_p(a+b) \geqslant \min(v_p(a), v_p(b))$, avec égalité si $v_p(a) \neq v_p(b)$.

Théorème C3.39

Pour tout $n \in \mathbb{Z} \setminus \{0\}$, il existe $\varepsilon \in \mathbb{Z}^\times = \{-1, 1\}$ et une famille $(\alpha_p)_{p \in \mathbb{P}}$ d'entiers naturels, à support fini, tels que

$$n = \varepsilon \prod_{p \in \mathbb{P}} p^{\alpha_p}.$$

De plus cette décomposition est unique : ε est le signe de n et $\forall p \in \mathbb{P}$, $\alpha_p = v_p(n)$.

Théorème C3.40

Soit $a, b \in \mathbb{Z}$. Alors
$$a \mid b \Leftrightarrow \forall p \in \mathbb{P},\ v_p(a) \leqslant v_p(b).$$

Proposition C3.41

Soit $n \in \mathbb{N}^*$, $a_1, \ldots, a_n \in \mathbb{Z}$ et $p \in \mathbb{P}$.

(i) $v_p\left(\bigwedge_{i=1}^{n} a_i\right) = \min\left\{v_p(a_i) \mid 1 \leqslant i \leqslant n\right\}$,

(ii) $v_p\left(\bigvee_{i=1}^{n} a_i\right) = \max\left\{v_p(a_i) \mid 1 \leqslant i \leqslant n\right\}$.

Méthodes

- Caractériser l'égalité de deux entiers par antisymétrie de la divisibilité.
- Utiliser les congruences modulo un entier.
- Déterminer PGCD, PPCM et coefficients de Bézout de deux entiers.
- Caractériser la coprimalité de deux entiers.
- Décomposer un entier en produit de facteurs premiers.