Chapitre 9. Arithmétique

1 Divisibilité

Définition 1.1. Soit $a, b \in \mathbb{Z}$
On dit que $\underline{a \text{ divise } b}$ (ou que b est un multiple de a) et on note $a \mid b$ si $\exists q \in \mathbb{Z} : b = aq$
On note $D(b)$ (resp. $D^+(b)$) l'ensemble des diviseurs (resp. de diviseurs ≥ 0) de b.

Proposition 1.2. Soit $a, b, c, d \in \mathbb{Z}$

* Si d divise a et b alors d divise toute combinaison $\mathbb{Z}$-linéaire de a et b, càd $\forall u, v \in \mathbb{Z}, d \mid au + bv$
* Règle des 2 parmi 3 :
  Si $a + b = c$ et que d divise deux de ces trois nombres, il divise le 3è
* Si a divise b et que $b \neq 0$, alors $|a| \leq |b|$

Proposition 1.3. Soit $a, b \in \mathbb{Z}$
LASSÉ :

(i) $a \mid b$ et $b \mid a$

(ii) $\exists u \in \mathbb{Z}^\times : b = au$

(iii) $b = \pm a$

Quand ces assertions sont vraies, on dit que a et b sont associés.

1.1 Division euclidienne dans $\mathbb{Z}$

Théorème 1.4. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$
Alors il existe un unique couple $(q, r) \in \mathbb{Z} \times [\![0, b-1]\!]$ tel que $a = bq + r$
q est le quotient de a par b
r est le reste dans la division de a par b

1.2 PGCD

Définition 1.5. Soit $a, b \in \mathbb{Z}$ non tous les deux nuls.
On définit $\text{pgcd}(a, b) = a \wedge b = \max(D(a) \cap D(b))$ le plus grand diviseur commun de a et b

Théorème 1.6. Soit $a, b \in \mathbb{Z}$ non tous les deux nuls.
On a $\langle a, b \rangle = (a \wedge b)\mathbb{Z}$
(où $\langle a, b \rangle = \mathbb{Z}a + \mathbb{Z}b = \{ua + vb \mid u, v \in \mathbb{Z}\}$)

Corollaire 1.7.

* La preuve montre que le PGCD de a et b est le plus grand diviseur commun de a et b au sens de la divisibilité : $a \wedge b$ est un multiple de tout diviseur commun de a et b
* On a en particulier $a \wedge b \in \langle a, b \rangle$, càd l'existence de $u, v \in \mathbb{Z}$ tels que $a \wedge b = au + bv$ (relation de Bézout)

Rappels : Algorithme d'Euclide et d'Euclide étendu :
Si a et b sont deux entiers (tous les deux > 0 pour fixer les idées) et que la division euclidienne est $a = bq + r$ alors $D(a) \cap D(b) = D(b) \cap D(r)$: tout diviseur commun à a et b est un diviseur commun à b et r (car $r = a - bq$ est une $CL_\mathbb{Z}$ de a et b) et réciproquement (car $a = bq + r$ est une $CL_\mathbb{Z}$ de b et r).
En particulier, $a \wedge b = \max(D(a) \cap D(b)) = \max(D(b) \cap D(r)) = b \wedge r$
L'algorithme d'Euclide exploite cette relation pour calculer rapidement $a \wedge b$

Définition 1.8. Soit $a_1, \ldots, a_n \in \mathbb{Z}$ non tous nuls.
On définit leur PGCD : $\text{pgcd}(a_1, \ldots, a_n) = a_1 \wedge \ldots \wedge a_n = \max(D(a_1) \cap \ldots \cap D(a_n))$

1.3 Entiers premiers entre eux

Définition 1.9. Soit $a, b \in \mathbb{Z}$ non tous deux nuls.
On dit que a et b sont premiers entre eux si $a \wedge b = 1$
On dit aussi (rarement) que a et b sont étrangers et on note (encore plus rarement) $a \perp b$

Théorème 1.10 (Lemme de Gauss). Soit $a, b, c \in \mathbb{Z}$
On suppose $a \mid bc$ et $a \perp b$. Alors $a \mid c$

Corollaire 1.11. Soit $a, b, c \in \mathbb{Z}$ tels que $\begin{cases} a \perp b \\ a, b \mid c \end{cases}$
Alors $ab \mid c$

Proposition 1.12. Soit $a, b \in \mathbb{Z}$ non tous deux nuls.

* Pour tout $k \in \mathbb{Z}^*$, $(ka) \wedge (kb) = k(a \wedge b)$
* En particulier, on peut trouver α, β premiers entre eux tels que :
  $\begin{cases} a = (a \wedge b)\alpha \\ b = (a \wedge b)\beta \end{cases}$

Lemme 1.13. Soit $x, y \in \mathbb{Z}$ et $k \in \mathbb{Z} \setminus \{0\}$
Alors $x \mid y \iff kx \mid ky$

Définition 1.14. Soit $a_1, \ldots, a_r \in \mathbb{Z}$ tous non nuls. On dit

* que $a_1, \ldots, a_r$ sont deux à deux premiers entre eux si $\forall i, j \in [\![1, r]\!], i \neq j \implies a_i \perp a_j$
* que $a_1, \ldots, a_r$ sont premiers entre eux dans leur ensemble si $a_1 \wedge \ldots \wedge a_r = 1$

Par exemple, $6, 10, 15$ sont premiers entre eux dans leur ensemble, mais pas deux à deux.

1.4 PPCM

Définition 1.15. Soit $a, b \in \mathbb{Z} \setminus \{0\}$
On définit le PPCM de a et b comme le plus petit entier ≥ 1 qui soit à la fois multiple de a et b
On le note $\operatorname{ppcm}(a, b)$ ou $a \vee b$

Proposition 1.16. Soit $a, b \in \mathbb{Z} \setminus \{0\}$
Les multiples communs à a et b sont les multiples de $a \vee b$

2 Nombres premiers

2.1 Généralités

Définition 2.1. Soit $n \geq 2$ un entier.
On dit que n est premier si $\forall a, b \in \mathbb{Z}, n = ab \implies (|a| = 1 \text{ ou } |b| = 1)$
On dit que n est composé s'il n'est pas premier.

Proposition 2.2. Soit p un nombre premier et $n \in \mathbb{Z}$
On a $n \perp p \iff p \nmid n$

Corollaire 2.3.

* p est premier avec tous les éléments de $[\![1, p-1]\!]$
* p est premier avec les nombres premiers $l \neq p$

Théorème 2.4 (Lemme d'Euclide). Soit p premier et $a_1, \ldots, a_r \in \mathbb{Z}$
Alors $p \mid a_1, \ldots, a_r$ si et seulement si $(p \mid a_1 \text{ ou } \ldots \text{ ou } p \mid a_r)$

2.2 Valuation p-adique

Définition 2.5. Soit p un nombre premier.
On définit la valuation p-adique

$$v_p : \begin{cases} \mathbb{Z} \to \mathbb{N} \cup \{+\infty\} \\ n \mapsto \begin{cases} \max\{k \in \mathbb{N} \mid p^k \mid n\} \text{ si } n \neq 0 \\ +\infty \text{ si } n = 0 \end{cases} \end{cases}$$

Lemme 2.6. Soit $n \in \mathbb{Z} \setminus \{0\}$ et p un nombre premier. Soit $k \in \mathbb{N}$
Alors $v_p(n) = k$ si et seulement s'il existe $n_0 \in \mathbb{Z}$ tel que $\begin{cases} n = p^k n_0 \\ p \nmid n_0 \end{cases}$

Théorème 2.7. Soit p un nombre premier, et $a, b \in \mathbb{Z}$

* On a $v_p(ab) = v_p(a) + v_p(b)$
* On a $v_p(a + b) \geq \min(v_p(a), v_p(b))$
* Si, en outre, $v_p(a) \neq v_p(b)$, alors $v_p(a + b) = \min(v_p(a), v_p(b))$

2.3 Décomposition en facteurs premiers

Théorème 2.8. Soit $n \in \mathbb{Z} \setminus \{0\}$
Alors il existe $\varepsilon \in \{-1, 1\}$, $r \in \mathbb{N}$, $p_1 < p_2 < ... < p_r$ des nombres premiers et $\alpha_1, ..., \alpha_r \in \mathbb{N}^*$ tels que

$$n = \varepsilon p_1^{\alpha_1} ... p_r^{\alpha_r} = \varepsilon \prod_{i=1}^{r} p_i^{\alpha_i}$$

Cette décomposition est unique.

Corollaire 2.9. Tout entier $n \geq 2$ possède un diviseur premier.

Corollaire 2.10. Soit $n, m \in \mathbb{Z} \setminus \{0\}$
On a $(n \wedge m)(n \vee m) = |n| \cdot |m|$

2.4 Infinitude des nombres premiers

Théorème 2.11. Il existe une infinité de nombres premiers.

3 Arithmétique et algèbre

3.1 Indicatrice d'Euler

Théorème 3.1. Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$
LASSÉ :

(i) $k \perp n$

(ii) $[k]_n$ est un inversible de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

(iii) $[k]_n$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$

Définition 3.2. On appelle fonction indicatrice d'Euler la fonction

$$\varphi : \begin{cases} \mathbb{N}^* \to \mathbb{N} \\ n \mapsto |\{k \in [\![1, n]\!] \mid k \perp n\}| \end{cases}$$

D'après le théorème $\varphi(n)$ est aussi le nombre d'inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ou le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$

3.2 Petit théorème de Fermat

Théorème 3.3. Soit p un nombre premier.
Alors pour tout $a \in \mathbb{Z}$:

* Si $p \nmid a$, on a $a^{p-1} \equiv 1 \pmod p$
* En général, $a^p \equiv a \pmod p$

Théorème 3.4 (Fermat - Euler)**.** Soit $n \geq 2$ et $a \in \mathbb{Z}$ tel que $a \perp n$
Alors $a^{\varphi(n)} \equiv 1 \pmod n$

3.3 Lemme chinois

Théorème 3.5 (Lemme chinois / théorème des restes chinois)**.** Soit $n; m \in \mathbb{N}^*$ premiers entre eux.
On a alors un isomorphisme d'anneaux

$$\varphi : \begin{cases} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ [k]_{nm} \mapsto ([k]_n, [k]_m) \end{cases}$$

Corollaire 3.6 (additif)**.** Soit $n, m \in \mathbb{N}^*$ premiers entre eux.
Alors le groupe $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est cyclique.

Corollaire 3.7 (multiplicatif)**.** Soit $n, m \in \mathbb{N}^*$ premiers entre eux.
On a un isomorphisme de groupes multiplicatifs $(\mathbb{Z}/nm\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$
En particulier, $\varphi(nm) = \varphi(n)\varphi(m)$ (indicatrice d'Euler)
On dit que φ est multiplicative (on a que pour tous n, m premiers entre eux, $\varphi(nm) = \varphi(n)\varphi(m)$)

Corollaire 3.8. Soit $n \in \mathbb{N}^*$ et $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ sa décomposition en facteurs premiers.
Alors

$$\begin{aligned} \varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) &= \prod_{i=1}^{r} (p_i - 1) p_i^{\alpha_i - 1} \\ &= \prod_{i=1}^{r} \left(\left(1 - \frac{1}{p_i}\right) p_i^{\alpha_i} \right) \\ &= n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \end{aligned}$$

Lemme 3.9. Soit A et B deux anneaux.
Si les anneaux A et B sont isomorphes, les groupes multiplicatifs $A^\times$ et $B^\times$ sont isomorphes.

Lemme 3.10. Soit R et S deux anneaux.
On a $(R \times S)^\times = R^\times \times S^\times$