ARITHMÉTIQUE

B. Landelle

Table des matières

La mention *entier* (sans précision) fait référence à entier naturel. L'anneau $(\mathbb{Z}, +, \times)$ est commutatif, intègre et on rappelle que pour tout idéal I de cet anneau, il existe un unique entier n tel que $\mathrm{I} = n\mathbb{Z}$.

I Arithmétique dans $\mathbb{Z}$

Soit $(a, b) \in \mathbb{Z}^2$. On a $\qquad a|b \iff b\mathbb{Z} \subset a\mathbb{Z} \iff b \in a\mathbb{Z}$

Comme $\mathrm{U}(\mathbb{Z}) = \{1, -1\}$, les entiers relatifs a et b sont associés si et seulement $a = \pm b$. Si a et b sont associés et sont des entiers naturels, alors $a = b$.

1 PGCD et PPCM

Définition 1. *Soit $(a, b) \in \mathbb{Z}^2$. On appelle* plus grand commun diviseur *de a et b noté $a \wedge b$ l'entier naturel d engendrant l'idéal $a\mathbb{Z} + b\mathbb{Z}$, i.e. tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.*

Remarque : Pour $(a, b) \in \mathbb{Z}^2$, on a $a \wedge b = b \wedge a$.

Proposition 1 (Relation de Bézout). *Soit $(a, b) \in \mathbb{Z}^2$. Il existe $(u, v) \in \mathbb{Z}^2$ tel que*

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

Démonstration. Immédiat par définition de $a \wedge b$. □

Remarque : Les entiers relatifs u et v de la relation de Bézout ne sont pas uniques. On a

$$\forall c \in \mathbb{Z} \qquad a(u - bc) + b(v + ac) = a \wedge b$$

Proposition 2. *Soit $(a, b) \in \mathbb{Z}^2$ et $d = a \wedge b$. On a d divise a et b et pour $c \in \mathbb{Z}$*

$$c|a \quad et \quad c|b \quad \Longrightarrow \quad c|d$$

Démonstration. Comme $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, on a en particulier $a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$, *i.e.* $d|a$ et $d|b$. Soit $(u, v) \in \mathbb{Z}^2$ tel que $d = au + bv$. Si $c|a$ et $c|b$, alors $c|au + bv = d$ ou aussi $a\mathbb{Z} \subset c\mathbb{Z}$ et $b\mathbb{Z} \subset c\mathbb{Z}$ d'où $a\mathbb{Z} + b\mathbb{Z} \subset c\mathbb{Z}$. □

Remarque : Cette propriété justifie l'appellation du *plus grand commun diviseur*.

Théorème 1 (Théorème d'Euclide). *Soit $(a, b) \in \mathbb{Z}^2$. Si $a = bq + r$ avec q et r dans $\mathbb{Z}$, alors on a*

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

Démonstration. On a $a \wedge b$ divise a et b donc divise b et $a - bq = r$ d'où divise $b \wedge r$. Puis on a $b \wedge r$ divise b et r donc divise b et $r + bq = a$ d'où divise $a \wedge b$. Ainsi, les entiers naturels $a \wedge b$ et $b \wedge r$ sont associés donc égaux. □

Commentaire : On peut alors envisager une implémentation de l'algorithme d'Euclide pour la détermination du pgcd de deux entiers.

Définition 2. *Soit $(a, b) \in \mathbb{Z}^2$. On appelle* plus petit commun multiple *de a et b noté $a \vee b$ l'entier naturel m engendrant l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$, i.e. tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.*

Proposition 3. *Soit $(a,b) \in \mathbb{Z}^2$ et $m = a \vee b$. On a a et b divisent m et pour $c \in \mathbb{Z}$*

$$a|c \quad et \quad b|c \quad \Longrightarrow \quad m|c$$

Démonstration. On a $m \in a\mathbb{Z}$ et $m \in b\mathbb{Z}$ puis $c \in a\mathbb{Z}$ et $c \in b\mathbb{Z}$ implique $c \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. □

Remarque : Cette propriété justifie l'appellation du *plus petit commun multiple*.

Définition 3. *Soit $(a_i)_{i\in[\![1\,;n]\!]} \in \mathbb{Z}^n$. On appelle* plus grand commun diviseur *des a_i noté $a_1 \wedge \ldots \wedge a_n$ l'entier naturel d engendrant l'idéal $\sum_{i=1}^{n} a_i\mathbb{Z}$ et* plus petit commun multiple *des a_i noté $a_1 \vee \ldots \vee a_n$ l'entier naturel m engendrant l'idéal $\bigcap_{i=1}^{n} a_i\mathbb{Z}$.*

2 Entiers premiers entre eux

Définition 4. *Deux entiers relatifs a et b sont dit* premiers entre eux *si $a \wedge b = 1$.*

Théorème 2 (Théorème de Bézout). *Soit $(a,b) \in \mathbb{Z}^2$. On a*

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

Démonstration. Le sens direct est immédiat d'après la relation de Bézout. Réciproquement, on a $a\mathbb{Z} + b\mathbb{Z} \supset 1\mathbb{Z} = \mathbb{Z}$ et l'autre inclusion étant immédiate, il s'ensuit que $a \wedge b$ et 1 sont des entiers associés donc égaux. □

Corollaire 1. *Soit $(a,b,c) \in \mathbb{Z}^3$. On a*

$$a \wedge bc = 1 \iff a \wedge b = 1 \quad et \quad a \wedge c = 1$$

Plus généralement, soit $(a, b_1, \ldots, b_n) \in \mathbb{Z}^{n+1}$. On a

$$a \wedge \prod_{i=1}^{n} b_i = 1 \iff \forall i \in [\![1\,;n]\!] \qquad a \wedge b_i = 1$$

Démonstration. Supposons $a \wedge bc = 1$. D'après le théorème de Bézout, il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bcv = 1$ d'où $a \wedge b = 1$ et $a \wedge c = 1$. Réciproquement, supposons que $a \wedge b = 1$ et $a \wedge c = 1$. Il existe $(u,v) \in \mathbb{Z}^2$ et $(k,\ell) \in \mathbb{Z}^2$ tels que $au + bv = 1$ et $ak + c\ell = 1$. Par suite, on a

$$au + bv(ak + c\ell) = 1 \iff a(u + bvk) + bcv\ell = 1$$

d'où $a \wedge bc = 1$. La généralisation se montre par récurrence. □

Corollaire 2. *Soit $(a,b) \in \mathbb{Z}^2$ et m, n entiers non nuls. On a*

$$a \wedge b = 1 \iff a^m \wedge b^n = 1$$

Démonstration. On utilise le corollaire 1. On suppose $a \wedge b = 1$. On en déduit $a \wedge b^n = 1$ puis $a^m \wedge b^n = 1$. Réciproquement, on a $(a \times a^{m-1}) \wedge b^n = 1$ d'où $a \wedge (b^{n-1} \times b) = 1$ d'où $a \wedge b = 1$. □

Corollaire 3. *Soit $(a,b,c) \in \mathbb{Z}^3$. On a*

$$a \wedge b = 1 \quad et \quad a|c \quad et \quad b|c \quad \Longrightarrow \quad ab|c$$

Plus généralement, soient $a_1, \ldots, a_n$ dans $\mathbb{Z}$ premiers entre eux deux à deux et $b \in \mathbb{Z}$. On a

$$\forall i \in [\![1\,;n]\!] \qquad a_i|b \quad \Longrightarrow \quad \prod_{i=1}^{n} a_i|b$$

Démonstration. Il existe $(k,\ell) \in \mathbb{Z}^2$ et $(u,v) \in \mathbb{Z}^2$ tels que $au+bv=1$, $c=ka$ et $c=\ell b$. On a

$$c = c(au+bv) = cau + cbv = \ell abu + kabv = ab(\ell u + kv)$$

□

Théorème 3. *Soit $(a,b) \in \mathbb{Z}^2$ avec a ou b non nul et $d \in \mathbb{N}^*$. On a*

$$a \wedge b = d \iff \exists!(a',b') \in \mathbb{Z}^2 \quad | \quad a = a'd \qquad b = b'd \quad \textit{et} \quad a' \wedge b' = 1$$

La généralisation se montre par récurrence.

Démonstration. Supposons $a \wedge b = d$. On a $d|a$ et $d|b$ d'où l'existence et unicité (d est non nul) de a' et b' tels que $a = a'd$ et $b = b'd$. Puis, d'après la relation de Bézout, il existe $(u,v) \in \mathbb{Z}^2$ tel que $au+bv=d$ d'où $a'u+b'v=1$ et d'après le théorème de Bézout, il s'ensuit que $a' \wedge b' = 1$. Réciproquement, on a $d|a$ et $d|b$ d'où $d|a \wedge b$. D'après le théorème de Bézout, il existe $(u,v) \in \mathbb{Z}^2$ tel que $a'u+b'v=1$ puis

$$d = d(a'u+b'v) = au+bv \in a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

ce qui prouve $a \wedge b | d$. Ainsi, les entiers naturels $a \wedge b$ et d sont associés donc égaux. □

Théorème 4 (Théorème de Gauss). *Soit $(a,b,c) \in \mathbb{Z}^3$. On a*

$$a \wedge b = 1 \quad \textit{et} \quad a|bc \quad \Longrightarrow \quad a|c$$

Démonstration. Il existe $(u,v) \in \mathbb{Z}^2$ tel que $au+bv=1$ et $k \in \mathbb{Z}$ tel que $bc=ka$. Par suite, on a

$$c = (au+bv)c = auc + bvc = auc + akv = a(uv+kv)$$

d'où le résultat. □

Corollaire 4. *Soit $(a,b,c) \in \mathbb{Z}^3$. On a*

$$a \wedge b = 1 \quad \Longrightarrow \quad a \wedge bc = a \wedge c$$

Démonstration. Posons $d = a \wedge bc$. On a $a \wedge c | a$ et $a \wedge c | bc$ d'où $a \wedge c | d$. Puis, on a $d|a$ et $d|bc$. Il reste à établir que $d|c$. Il existe $k \in \mathbb{Z}$ tel que $a = kd$ puis, d'après le corollaire 1, comme $b \wedge kd = 1$, alors $b \wedge d = 1$ et d'après le théorème de Gauss, comme $d|bc$, alors $d|c$ et par conséquent $d | a \wedge c$. Ainsi Les entiers $a \wedge bc$ et $a \wedge c$ sont associés et donc égaux.

Variante. Pour établir $d|c$, on peut aussi invoquer le théorème de Bézout : il existe $(u,v) \in \mathbb{Z}^2$ tel que $au+bv=1$ d'où

$$c = c(au+bv) = acu + bcv \in a\mathbb{Z} + bc\mathbb{Z} = d\mathbb{Z}$$

□

3 Nombres premiers

Définition 5. *Un entier $p \geqslant 2$ est dit* premier *s'il admet comme seuls diviseurs positifs 1 et lui-même.*

Notations : On note $\mathcal{P} = \{2,3,5,7,11,\ldots\}$ l'ensemble des nombres premiers.
Vocabulaire : Un nombre qui n'est pas premier est dit *composé*.

Proposition 4. *Soit $a \in \mathbb{Z}$ et p un nombre premier. On a*

$$p \nmid a \iff p \wedge a = 1$$

Démonstration. On a $p \wedge a$ diviseur de p d'où $p \wedge a \in \{1, p\}$. Si $p \wedge a = p$, alors $p|a$. Réciproquement, si $p|a$, alors $p|p \wedge a$ d'où $p \wedge a \neq 1$. Par négation, le résultat suit. □

Proposition 5. *Soit $a \in \mathbb{Z}$, n entier non nul et p un nombre premier. On a*

$$p|a \iff p|a^n$$

Démonstration. Avec le résultat de la proposition précédente et le corollaire 2, on obtient :

$$p \nmid a \iff p \wedge a = 1 \iff p \wedge a^n = 1 \iff p \nmid a^n$$

d'où le résultat par négation. □

Proposition 6 (Lemme d'Euclide). *Soit $(a, b) \in \mathbb{Z}^2$ et p un nombre premier. On a*

$$p|ab \quad \Longrightarrow \quad p|a \quad ou \quad p|b$$

Démonstration. On a

$$p \nmid ab \iff p \wedge ab = 1 \iff p \wedge a = 1 \quad \text{et} \quad p \wedge b = 1 \iff p \nmid a \quad \text{et} \quad p \quad \text{et} \quad \nmid b$$

Le résultat suit par négation. □

Définition 6. *Soit n entier non nul et p un nombre premier. On appelle* p-valuation *de n l'entier noté $v_p(n)$ défini par*

$$v_p(n) = \max\left\{k \in \mathbb{N} \mid p^k \text{ divise } n\right\}$$

Remarque : L'ensemble $\left\{k \in \mathbb{N} \mid p^k \text{ divise } n\right\}$ est une partie non vide de $\mathbb{N}$ puisqu'il contient 0 et majorée car sinon, on peut trouver k entier tel que $p^k > n$ et $p^k|n$ ce qui est absurde si n non nul.

Proposition 7. *Soit n entier non nul et p un nombre premier. Il existe a entier non nul premier avec p tel que*

$$n = p^{v_p(n)}a$$

Démonstration. Par définition de la valuation, on a $p^{v_p(n)}|n$ d'où l'existence de a entier non nul tel que $n = p^{v_p(n)}a$ et $p \nmid a$ par maximalité de la valuation d'où $a \wedge p = 1$. □

Théorème 5. *Soit n entier avec $n \geqslant 2$. Alors, on a $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec r entier non nul, les p_i des nombres premiers deux à deux distincts et les α_i des entiers non nuls. Cette décomposition est unique à l'ordre près.*

Démonstration. En annexe. □

Remarques : (1) Les α_i sont les p_i-valuations de n.
(2) La décomposition est unique si on ordonne les facteurs premiers dans la décomposition en produit. On peut donc parler de *la* décomposition.
(3) Pour n entier non nul, on peut encore écrire

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

En effet, la famille $(v_p(n))_{p \in \mathcal{P}}$ est presque nulle et il s'agit donc d'un produit fini. Si $n = 1$, toutes les p-valuations sont nulles.

Théorème 6. *Soient m et n des entiers non nuls. On a*

1. $\forall p \in \mathcal{P} \qquad v_p(nm) = v_p(n) + v_p(m)$
2. $m|n \iff \forall p \in \mathcal{P} \qquad v_p(m) \leqslant v_p(n)$

Démonstration. 1. Soit p premier. On note $n = p^\alpha a$ et $m = p^\beta b$ avec a et b entiers non nuls tels que $p \wedge a = p \wedge b = 1$. Ainsi, on a $nm = p^{\alpha+\beta}ab$ avec $p \wedge ab = 1$ d'où $p \nmid ab$ et par suite $v_p(nm) = \alpha + \beta$.
2. Si $m|n$, alors $n = km$ avec k entier non nul et le résultat découle du premier point. Réciproquement, on a

$$n = \prod_{p\in\mathcal{P}} p^{v_p(n)} = \underbrace{\prod_{p\in\mathcal{P}} p^{v_p(m)}}_{=m} \times \underbrace{\prod_{p\in\mathcal{P}} p^{v_p(n)-v_p(m)}}_{\in\mathbb{N}^*}$$

d'où le résultat. □

Application : Montrons que $\sqrt{2}$ est irrationnel. S'il existe a et b entiers non nuls tels que $\sqrt{2} = \dfrac{a}{b}$, alors on trouve $a^2 = 2b^2$ puis $2v_2(a) = 1 + 2v_2(b)$ ce qui est absurde (un entier pair égal à un entier impair). La preuve historique ne s'appuie pas sur les valuations. On suppose l'écriture de la fraction irréductible à savoir a et b premiers entre eux. Comme $a^2 = 2b^2$, on a $2|a^2$ d'où $2|a$, *i.e.* $a = 2a'$ avec a' entier puis $4a'^2 = 2b^2$, c'est-à-dire $2a'^2 = b^2$ d'où $2|b^2$ et donc $2|b$ ce qui contredit le fait que $a \wedge b = 1$.

Corollaire 5. *Soit n entier avec $n \geqslant 2$ et $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ sa décomposition en facteurs premiers avec les α_i entiers non nuls. L'ensemble des diviseurs positifs de n noté $\mathcal{D}_n$ est*

$$\mathcal{D}_n = \left\{ \prod_{i=1}^{r} p_i^{\beta_i} \mid \forall i \in [\![1\,;\, r]\!] \quad \beta_i \in [\![0\,;\, \alpha_i]\!] \right\}$$

Démonstration. Conséquence immédiate du théorème précédent.

□

Remarque : On peut aussi écrire pour n entier non nul

$$\mathcal{D}_n = \left\{ \prod_{p\in\mathcal{P}} p^{\beta_p}, \forall p \in \mathcal{P} \quad \beta_p \in [\![0\,;\, v_p(n)]\!] \right\}$$

Théorème 7. *Soient a et b des entiers non nuls avec $a = \prod_{p\in\mathcal{P}} p^{v_p(a)}$ et $b = \prod_{p\in\mathcal{P}} p^{v_p(b)}$ leurs décompositions en facteurs premiers. On a*

$$a \wedge b = \prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))} \qquad a \vee b = \prod_{p\in\mathcal{P}} p^{\max(v_p(a),v_p(b))} \quad \text{et} \quad (a \wedge b)(a \vee b) = ab$$

Démonstration. Notons $c = \prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))}$ et $d = \prod_{p\in\mathcal{P}} p^{\max(v_p(a),v_p(b))}$. On utilise l'équivalence fournie dans le théorème 6. On a $a \wedge b|a$ et $a \wedge b|b$ d'où

$$\forall p \in \mathcal{P} \qquad v_p(a \wedge b) \leqslant v_p(a) \quad \text{et} \quad v_p(a \wedge b) \leqslant v_p(b)$$

et par suite $\qquad \forall p \in \mathcal{P} \qquad v_p(a \wedge b) \leqslant \min(v_p(a), vp_p(b))$

ce qui prouve $a \wedge b | c$. Puis, comme on a

$$\forall p \in \mathcal{P} \qquad v_p(c) \leqslant v_p(a) \quad \text{et} \quad v_p(c) \leqslant v_p(b)$$

il s'ensuit $c|a$ et $c|b$ d'où $c|a \wedge b$ ce qui prouve que $a \wedge b$ et c sont des entiers associés donc égaux. Ensuite, on a $a|a \vee b$ et $b|a \vee b$ d'où

$$\forall p \in \mathcal{P} \qquad v_p(a) \leqslant v_p(a \vee b) \quad \text{et} \quad v_p(b) \leqslant v_p(a \vee b)$$

puis

$$\forall p \in \mathcal{P} \qquad \max(v_p(a), v_p(b)) \leqslant v_p(a \vee b)$$

ce qui prouve $d|a \vee b$. Par ailleurs, on a

$$\forall p \in \mathcal{P} \qquad v_p(a) \leqslant v_p(d) \quad \text{et} \quad v_p(b) \leqslant v_p(d)$$

d'où $a|d$ et $b|d$ et par conséquent $a \vee b|d$ et on conclut que d et $a \vee b$ sont des entiers associés donc égaux. La dernière égalité résulte de

$$\forall p \in \mathcal{P} \qquad \min(v_p(a), v_p(b)) + \max(v_p(a), v_p(b)) = v_p(a) + v_p(b)$$

□

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

1 Opérations

Proposition 8. *Soit n entier non nul. La relation de congruence modulo n est compatible avec l'addition et la multiplication, i.e.*

$$\forall (x, y, u, v) \in \mathbb{Z}^4 \qquad \begin{cases} x \equiv u \ [n] \\ y \equiv v \ [n] \end{cases} \implies \begin{cases} x + y \equiv u + v \ [n] \\ xy \equiv uv \ [n] \end{cases}$$

Démonstration. Soit $(k, \ell) \in \mathbb{Z}^2$ tel que $x = u + kn$ et $y = v + \ell n$. Par suite

$$x + y = u + v + n(k + \ell) \quad \text{et} \quad xy = (u + kn)(v + \ell n) = uv + n(\ell u + kv + nk\ell)$$

Le résultat suit. □

Définition 7. *Soit n entier non nul. On munit $\mathbb{Z}/n\mathbb{Z}$ des opérations $+$ et $\times$ définies par*

$$\forall (x, y) \in \mathbb{Z}^2 \qquad \bar{x} + \bar{y} = \overline{x + y} \quad \text{et} \quad \bar{x} \times \bar{y} = \overline{xy}$$

Remarque : D'après la proposition précédente, ces opérations sont bien définies puisque les résultats ne dépendent pas des représentants choisis pour chaque classe.

2 Structure

Théorème 8. *Soit n entier non nul. Le triplet $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif de neutres $\bar{0}$ et $\bar{1}$.*

Démonstration. L'ensemble $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien de neutre $\bar{0}$. Soit $(x, y, z) \in \mathbb{Z}^3$. On a

$$\bar{x}(\bar{y}\bar{z}) = \bar{x}\overline{yz} = \overline{xyz} = \overline{xy}\bar{z} = (\bar{x}\bar{y})\bar{z}$$

puis $\quad \bar{x}\bar{1} = \bar{x} \quad$ et $\quad \bar{x}(\bar{y} + \bar{z}) = \bar{x}\overline{y + z} = \overline{x(y + z)} = \overline{xy + xz} = \overline{xy} + \overline{xz} = \bar{x}\bar{y} + \bar{x}\bar{z}$

Enfin

$$\bar{x}\bar{y} = \overline{xy} = \overline{yx} = \bar{y}\bar{x}$$

ce qui prouve que la loi $\times$ est commutative et complète les vérifications. □

Remarque : Si $n = 1$, on a $\mathbb{Z}/1\mathbb{Z} = \{\bar{0}\}$ anneau nul et $\bar{1} = \bar{0}$.

Proposition 9. *Soit n entier non nul. L'application $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, x \mapsto \bar{x}$ est un morphisme d'anneaux avec* $\operatorname{Im}\varphi = \mathbb{Z}/n\mathbb{Z}$ *et* $\operatorname{Ker}\varphi = n\mathbb{Z}$.

Démonstration. Par définition de l'addition et la multiplication dans $\mathbb{Z}/n\mathbb{Z}$, l'application φ est un morphisme d'anneaux. L'image et le noyau coïncident avec les notions du morphisme de groupe d'où le résultat. □

Proposition 10. *Soit n entier non nul et $x \in \mathbb{Z}$. Dans $\mathbb{Z}/n\mathbb{Z}$, on a $k\bar{x} = \overline{kx}$ pour $k \in \mathbb{Z}$ et $\bar{x}^k = \overline{x^k}$ pour $k \in \mathbb{N}$.*

Démonstration. Considérant le morphisme d'anneaux $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, x \mapsto \bar{x}$. Pour $x \in \mathbb{Z}$, on a

$$\forall k \in \mathbb{Z} \qquad k\bar{x} = k\varphi(x) = \varphi(kx) = \overline{kx} \quad \text{et} \quad \forall k \in \mathbb{N} \qquad \bar{x}^k = \varphi(x)^k = \varphi(x^k) = \overline{x^k}$$

□

Théorème 9. *Soit n entier non nul. On a*

$$\mathrm{U}(\mathbb{Z}/n\mathbb{Z}) = \left\{\bar{k}, k \in \mathbb{Z} \mid k \wedge n = 1\right\}$$

Démonstration. Soit $k \in \mathbb{Z}$. On a

$$\bar{k} \in \mathrm{U}(\mathbb{Z}/n\mathbb{Z}) \iff \exists \bar{\ell} \in \mathbb{Z}/n\mathbb{Z} \quad | \quad \bar{k}\bar{\ell} = \bar{1} \iff \exists \ell \in \mathbb{Z} \quad | \quad k\ell \equiv 1\ [n]$$
$$\iff \exists (\ell, q) \in \mathbb{Z}^2 \quad | \quad k\ell + nq = 1$$

Le résultat suit d'après le théorème de Bézout. □

Remarques : (1) Les inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont les générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
(2) On peut aussi écrire pour n entier non nul

$$\mathrm{U}(\mathbb{Z}/n\mathbb{Z}) = \left\{\bar{k}, k \in [\![1\,;\,n]\!] \mid k \wedge n = 1\right\}$$

Exemple : Avec l'algorithme d'Euclide, on peut déterminer un inverse dans $\mathbb{Z}/n\mathbb{Z}$. On a $\overline{14} \in \mathrm{U}(\mathbb{Z}/37\mathbb{Z})$. Puis, on trouve

$$37 = 14 \times 2 + 9 \qquad 14 = 9 \times 1 + 5 \qquad 9 = 5 \times 1 + 4 \qquad 5 = 4 \times 1 + 1$$

d'où $\quad 1 = 5 - 4 \times 1 \qquad 4 = 9 - 5 \times 1 \qquad 5 = 14 - 9 \times 1 \quad$ et $\quad 9 = 37 - 14 \times 2$

et

$$1 = (14 - 9 \times 1) - (9 - 5 \times 1) \times 1 = (14 - (37 - 14 \times 2)) - (37 - 14 \times 2 - (14 - (37 - 14 \times 2) \times 1) \times 1$$

d'où $\qquad 1 = -3 \times 37 + 8 \times 14$

et par conséquent $\qquad \overline{14}^{-1} = \bar{8}$

Corollaire 6. *Soit p entier non nul. On a*

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

Démonstration. L'anneau $\mathbb{Z}/\mathbb{Z}$ est nul et n'est donc pas un corps. On suppose $p \geqslant 2$. On rappelle l'égalité $\mathbb{Z}/p\mathbb{Z} = \left\{\bar{k}, k \in [\![0\,;\,p-1]\!]\right\}$. On a

$$\mathbb{Z}/p\mathbb{Z} \text{ corps} \iff \mathrm{U}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\} \iff \forall k \in [\![1\,;\,p-1]\!] \quad k \wedge p = 1 \iff p \text{ premier}$$

□

Notation : Pour p un nombre premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

3 Théorème chinois (ou des restes chinois)

Soient m et n des entiers non nuls. Pour $k \in \mathbb{Z}$, on note respectivement $\bar{k}$, $\widehat{k}$ et $\dot{k}$ les classes d'équivalence de k dans $\mathbb{Z}/mn\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$.

Théorème 10. *Soient m et n des entiers non nuls. Si m et n sont premiers entre eux, alors l'application*

$$\pi : \begin{cases} \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \quad \bar{k} \quad \longmapsto (\widehat{k}, \dot{k}) \end{cases}$$

est un isomorphisme d'anneaux.

Démonstration. Soit $(k, \ell) \in \mathbb{Z}^2$. L'application π est bien définie car

$$k \equiv \ell \ [mn] \quad \Longrightarrow \quad k \equiv \ell \ [m] \quad \text{et} \quad k \equiv \ell \ [n]$$

Ainsi, pour $\bar{x} \in \mathbb{Z}/mn\mathbb{Z}$, on choisit $x \in \bar{x} \cap [\![0 \,;\, mn-1]\!]$ et on peut définir l'application

$$\bar{x} \mapsto x \mapsto (\widehat{x}, \dot{x})$$

le choix de x comme représentant de $\bar{x}$ étant sans incidence d'après la remarque préliminaire. On a $\pi(\bar{1}) = (\widehat{1}, \dot{1})$ puis sans difficulté

$$\pi(\bar{k} + \bar{\ell}) = \pi(\overline{k+\ell}) = \ldots = \pi(\bar{k}) + \pi(\bar{\ell})$$

et

$$\pi(\bar{k}\bar{\ell}) = \pi(\overline{k\ell}) = \ldots = \pi(\bar{k})\pi(\bar{\ell})$$

Enfin $\quad \pi(\bar{k}) = (\widehat{0}, \dot{0}) \iff k \equiv 0 \ [m] \quad \text{et} \quad k \equiv 0 \ [n] \iff k \in m\mathbb{Z} \cap n\mathbb{Z}$

Or, on sait $m \wedge n = 1$ d'où $m \vee n = mn$ et on obtient

$$\bar{k} \in \operatorname{Ker} \pi \iff k \in mn\mathbb{Z} \iff \bar{k} = \bar{0}$$

Enfin, avec l'égalité $\quad \operatorname{Card} \mathbb{Z}/mn\mathbb{Z} = mn = \operatorname{Card} \mathbb{Z}/m\mathbb{Z} \times \operatorname{Card} \mathbb{Z}/n\mathbb{Z}$

on conclut que π est bijectif et qu'il s'agit donc d'un isomorphisme. □

Application : Résolution de $\begin{cases} x \equiv a \ [m] \\ x \equiv b \ [n] \end{cases}$ avec $m \wedge n = 1$. De manière équivalente, on résout

$$\pi(\bar{x}) = (\widehat{a}, \dot{b}) = a(\widehat{1}, \dot{0}) + b(\widehat{0}, \dot{1})$$

D'après la relation de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $um + vn = 1$ et on remarque

$$\pi(\overline{um}) = (\widehat{0}, \dot{1}) \quad \text{et} \quad \pi(\overline{vn}) = (\widehat{1}, \dot{0})$$

L'ensemble des solutions est donc $\{avn + bum + kmn, k \in \mathbb{Z}\}$.

Exemple : Résolution de $\begin{cases} x \equiv 2 \ [14] \\ x \equiv 5 \ [37] \end{cases}$.

On trouve $\quad \{2 \times -3 \times 37 + 5 \times 8 \times 14 + k \times 14 \times 37, k \in \mathbb{Z}\}$

Remarque : Avec la relation de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $um + vn = 1$ et on a remarqué

$$\pi(\overline{um}) = (\widehat{0}, \dot{1}) \quad \text{et} \quad \pi(\overline{vn}) = (\widehat{1}, \dot{0})$$

puis $$\pi(\overline{avn+bum}) = a\pi(\overline{vn}) + b\pi(\overline{um}) = (\widehat{a}, \dot{b})$$

Ceci prouve la surjectivité de π et par égalité des cardinaux, on pourrait conclure à la bijectivité de π sans passer par l'injectivité ou aussi conclure uniquement avec injectivité et surjectivité.

Théorème 11. *Soient $n_1, \dots, n_r$ des entiers non nuls premiers entre eux deux à deux et $n = \prod_{i=1}^{r} n_i$. L'application*

$$\pi : \begin{cases} \mathbb{Z}/n\mathbb{Z} \longrightarrow \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \\ \overline{k}^{[n]} \longmapsto \left(\overline{k}^{[n_1]}, \dots, \overline{k}^{[n_r]}\right) \end{cases}$$

est un isomorphisme d'anneaux.

Démonstration. On procède par récurrence sur r. Le cas $r = 1$ est trivial. Supposons le résultat vrai au rang $r - 1 \geqslant 1$. D'après le corollaire 1, on a

$$\forall k \in [\![1 ; r-1]\!] \qquad n_r \wedge n_k = 1 \iff n_r \wedge \prod_{i=1}^{r-1} n_i = 1$$

On applique alors le théorème chinois avec $\prod_{i=1}^{r-1} n_i$ et n_r et l'hérédité suit. □

Corollaire 7. *Soient m et n des entiers non nuls. Si m et n sont premiers entre eux, alors on a l'isomorphisme de groupes multiplicatifs*

$$\mathrm{U}(\mathbb{Z}/mn\mathbb{Z}) \simeq \mathrm{U}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = \mathrm{U}(\mathbb{Z}/m\mathbb{Z}) \times \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$$

Démonstration. La dernière égalité résulte du théorème sur les inversibles d'un produit d'anneaux. Le morphisme d'anneaux π envoie un inversible sur un inversible d'où

$$\pi(\mathrm{U}(\mathbb{Z}/mn\mathbb{Z})) \subset \mathrm{U}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$$

De même, comme l'application réciproque π^{-1} réalise un isomorphisme d'anneaux de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sur $\mathbb{Z}/mn\mathbb{Z}$, on obtient

$$\pi^{-1}(\mathrm{U}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})) \subset \mathrm{U}(\mathbb{Z}/mn\mathbb{Z})$$

Ainsi, notant $\pi^* : \mathrm{U}(\mathbb{Z}/mn\mathbb{Z}) \to \mathrm{U}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}), \bar{k} \mapsto \pi(\bar{k})$, cette application est bien définie et réalise une bijection. Enfin, c'est un morphisme de groupes multiplicatifs par héritage du morphisme d'anneaux et constitue donc un isomorphisme de groupes. □

Corollaire 8. *Soient $n_1, \dots, n_r$ des entiers non nuls premiers entre eux deux à deux et $n = \prod_{i=1}^{r} n_i$. On a l'isomorphisme de groupes multiplicatifs*

$$\mathrm{U}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{U}(\prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}) = \prod_{i=1}^{r} \mathrm{U}(\mathbb{Z}/n_i\mathbb{Z})$$

Démonstration. On procède par récurrence sur r. Le cas $r = 1$ est trivial. Supposons le résultat vrai au rang $r - 1 \geqslant 1$. D'après le corollaire 1, on a

$$\forall k \in [\![1 ; r-1]\!] \qquad n_r \wedge n_k = 1 \iff n_r \wedge \prod_{i=1}^{r-1} n_i = 1$$

On applique alors le corollaire précédent avec $\prod_{i=1}^{r-1} n_i$ et n_r et l'hérédité suit. □

4 Indicatrice d'Euler, applications

Définition 8. *On appelle fonction* indicatrice d'Euler *la fonction* $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ *définie par*

$$\forall n \in \mathbb{N}^* \qquad \varphi(n) = \text{Card}\,\{k \in [\![\,1\,;\,n\,]\!] \mid k \wedge n = 1\}$$

Remarque : Pour n entier non nul, $\varphi(n)$ est égal au nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ ou encore $\varphi(n) = \text{Card}\,\text{U}(\mathbb{Z}/n\mathbb{Z})$. En particulier, on a $\varphi(1) = 1$.

Théorème 12. *Soit* p *un nombre premier et* α *entier non nul. On a*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

Démonstration. Soit $k \in [\![\,1\,;\,p^\alpha\,]\!]$. On a

$$k \wedge p^\alpha \neq 1 \iff k \wedge p \neq 1 \iff p|k \iff k \in \{p, 2p, \ldots, p^{\alpha-1}p\}$$

Le résultat suit. □

Théorème 13. *Soient* m *et* n *deux entiers non nuls premiers entre eux. Alors*

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Démonstration. Conséquence du corollaire 7. □

Corollaire 9. *Soient* $n_1, \ldots, n_r$ *des entiers non nuls premiers entre eux deux à deux. Alors*

$$\varphi\left(\prod_{i=1}^{r} n_i\right) = \prod_{i=1}^{r} \varphi(n_i)$$

Démonstration. Conséquence du corollaire 8. □

Remarque : On peut aussi l'établir par récurrence à partir du théorème 13.

Théorème 14. *Soit* n *entier avec* $n \geqslant 2$ *se décomposant en* $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ *avec les* p_i *des nombres premiers deux à deux distincts et les* α_i *des entiers non nuls. On a*

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Démonstration. Pour $(i, j) \in [\![\,1\,;\,r\,]\!]^2$, on a $p_i \wedge p_j = 1$ (puisque $p_i \wedge p_j \in \{1, p_i\} \cap \{1, p_j\}$) d'où $p_i^{\alpha_i} \wedge p_j^{\alpha_j} = 1$. D'après le corollaire 9 et le théorème 12, il vient

$$\varphi(n) = \varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{r} \left[p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)\right]$$

Le résultat suit. □

Théorème 15 (Théorème d'Euler). *Soit* $a \in \mathbb{Z}$ *et* n *entier non nul avec* $a \wedge n = 1$. *Alors*

$$a^{\varphi(n)} \equiv 1\ [n]$$

Démonstration. On a $\bar{a} \in \text{U}(\mathbb{Z}/n\mathbb{Z})$ et $\varphi(n)$ est l'ordre du groupe $\text{U}(\mathbb{Z}/n\mathbb{Z})$. Le résultat suit. □

Remarques : (1) En particulier, si p premier, on a $\varphi(p) = p - 1$ et on retrouve le *petit théorème de Fermat* : si $a \wedge p = 1$, alors $a^{p-1} \equiv 1\ [p]$ et pour tout $a \in \mathbb{Z}$, $a^p \equiv a\ [p]$ (le résultat vaut toujours si $p|a$ car $p|a^p$ dans ce cas). Ce résultat est faux en général si p n'est pas premier : on a $3^4 \equiv 1 \not\equiv 3\ [4]$.

(2) Le résultat du théorème d'Euler est faux en général si $a \wedge n \neq 1$. Dans $\mathbb{Z}/4\mathbb{Z}$, on a $\varphi(4) = 2$ puis $2^2 \equiv 0 \not\equiv 1\ [4]$. On voit aussi $2^3 \equiv 0 \not\equiv 2\ [4]$ donc on n'a pas non plus $a^{\varphi(n)+1} \equiv a\ [n]$.

III Fonctions multiplicatives (hors-programme)

1 Définitions

Définition 9. *Une fonction* arithmétique *est une fonction* $f : \mathbb{N}^* \to \mathbb{C}$.

Définition 10. *Une fonction arithmétique* f *est dite* multiplicative *si*
- $f(1) = 1$;
- $\forall (m,n) \in (\mathbb{N}^*)^2 \quad m \wedge n = 1 \Longrightarrow f(mn) = f(m)f(n)$.

Exemples : 1. La fonction indicatrice d'Euler φ est multiplicative d'après le théorème chinois.
2. La fonction μ de *Möbius* :

$$\forall n \in \mathbb{N}^* \qquad \mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts} \\ 0 & \text{sinon} \end{cases}$$

Si n ou m est égal à 1 ou si n ou m contient des facteurs carrés, alors $\mu(nm) = \mu(n)\mu(m)$. Supposons n et m distincts de 1 et respectivement produits de r et s nombres premiers distincts. Si $n \wedge m = 1$, alors nm est le produit de $r + s$ nombres premiers distincts d'où

$$\mu(nm) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(n)\mu(m)$$

Définition 11. *Une fonction arithmétique* f *est dite* complètement multiplicative *si*
- $f(1) = 1$;
- $\forall (m,n) \in (\mathbb{N}^*)^2 \qquad f(mn) = f(m)f(n)$.

Exemples : 1. Les fonctions puissances $n \mapsto n^k$ avec k entier sont complètement mutliplicatives.
2. La fonction λ de Liouville avec $\lambda : n \mapsto (-1)^{\sum_{p\in\mathcal{P}} v_p(n)}$ l'est aussi.

2 Convolution

Définition 12. *La* convolution de Dirichlet *de deux fonctions arithmétiques* f *et* g *est la fonction notée* $f * g$ *définie par*

$$\forall n \in \mathbb{N}^* \qquad (f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

Proposition 11. *Soient* f, g, h *des fonctions arithmétiques. On a*

$$\forall n \in \mathbb{N}^* \qquad (f * g)(n) = \sum_{(a,b)\in(\mathbb{N}^*)^2,\ ab=n} f(a)g(b)$$

et

$$\forall n \in \mathbb{N}^* \qquad ((f \star g) \star h)(n) = \sum_{(a,b,c)\in(\mathbb{N}^*)^3,\ abc=n} f(a)g(b)h(c)$$

Démonstration. Soit $n \in \mathbb{N}^*$. On note $\mathcal{C}_n = \{(a,b) \in (\mathbb{N}^*)^2,\ ab = n\}$. L'application $\mathcal{D}_n \to \mathcal{C}_n, d \mapsto (d, n/d)$ réalise une bijection d'où

$$\sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{(a,b)\in(\mathbb{N}^*)^2,\ ab=n} f(a)g(b)$$

puis

$$((f*g)*h)(n) = \sum_{(d,c)\in(\mathbb{N}^*)^2,\ dc=n} (f*g)(d)h(c)$$
$$= \sum_{(d,c)\in(\mathbb{N}^*)^2,\ dc=n} \left(\sum_{(a,b)\in(\mathbb{N}^*)^2, ab=d} f(a)g(b)h(c) \right) = \sum_{(a,b,c)\in(\mathbb{N}^*)^3, abc=n} f(a)g(b)h(c)$$

□

Théorème 16. *L'ensemble des fonctions arithmétiques muni des lois + et $*$ possède une structure d'anneau commutatif avec pour neutre $\delta = \mathbb{1}_{\{1\}}$.*

Démonstration. Les lois + et $*$ sont des lois de composition interne sur l'ensemble des fonctions arithmétiques. D'après les égalités établies dans la proposition précédente, la loi $*$ est commutative et associative. Les autres propriétés se vérifient sans difficulté. □

Proposition 12. *Soit μ la fonction de Möbius. Notant $\mathbb{1}$ la fonction arithmétique constante égale à 1, on a*

$$\mathbb{1} * \mu = \delta$$

Démonstration. On a clairement $(\mathbb{1}*\mu)(1) = 1$. Pour $n \geqslant 2$, notant r le nombre de facteurs premiers de n avec $r \geqslant 1$, pour $d|n$, soit d admet un facteur carré et dans ce cas $\mu(d) = 0$, sinon d est le produit de k termes pris parmi les r facteurs premiers de n et dans ce cas $\mu(d) = (-1)^k$. Il s'ensuit

$$(\mathbb{1}*\mu)(n) = \sum_{d|n} \mu(d) = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = (1-1)^r = 0$$

d'où le résultat. □

Théorème 17 (Inversion de Möbius). *Soit f une fonction arithmétique et $g = f * \mathbb{1}$. On a*

$$f = g * \mu$$

Démonstration. Par associativité de $*$, on a

$$f = f*\delta = f*(\mathbb{1}*\mu) = (f*\mathbb{1})*\mu = g*\mu$$

□

Exemple : On peut établir $\sum_{d|n} \varphi(d) = n$ pour $n \in \mathbb{N}^*$ ce qui équivaut à $\varphi * \mathbb{1} = \mathrm{id}$. Par inversion de Möbius, on en déduit $\varphi = \mathrm{id} * \mu$, c'est-à-dire

$$\forall n \in \mathbb{N}^* \qquad \varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$$

Proposition 13. *Soient m et n dans $\mathbb{N}^*$ premiers entre eux. L'application*

$$\pi : \begin{cases} \mathcal{D}_n \times \mathcal{D}_m & \longrightarrow \mathcal{D}_{mn} \\ (d_1, d_2) & \longmapsto d_1 d_2 \end{cases}$$

réalise une bijection de $\mathcal{D}_n \times \mathcal{D}_m$ sur $\mathcal{D}_{mn}$.

Démonstration. L'application est bien définie : si $d_1|n$ et $d_2|m$, alors $d_1 d_2 | mn$. Soient (d_1, d_2), (d_1', d_2') dans $\mathcal{D}_n \times \mathcal{D}_m$ tels que $d_1 d_2 = d_1' d_2'$. On a $d_1 | d_1' d_2'$ et $d_1 \wedge d_2' = 1$ puisque $d_1 \wedge m = 1$ et $d_2' | m$. D'après le lemme de Gauss, il s'ensuit $d_1 | d_1'$ et de même $d_2 | d_2'$. Par symétrie des rôles, on obtient que d_1, d_1' sont des entiers associés donc égaux et de même avec d_2, d_2' d'où l'injectivité

de π. Soit $d \in \mathcal{D}_{mn}$. On pose $d_1 = d \wedge n$ et $d_2 = d \wedge m$. On a $d_1 | n$ et $d_2 | m$ et comme $n \wedge m = 1$, alors $d_1 \wedge d_2 = 1$. De plus, on a $d_1 | d$ et $d_2 | d$ d'où $d_1 d_2 | d$. Puis, d'après la relation de Bézout, on dispose de a, b, u, v dans $\mathbb{Z}$ tels que

$$d_1 = ad + bn \qquad d_2 = ud + vm$$

d'où
$$d_1 d_2 = d(aud + avm + bu) + mnbv$$

Or, on a $d | mn$ d'où $d | d_1 d_2$ et par conséquent, les entiers d et $d_1 d_2$ sont associés donc égaux. Ainsi, l'application π est surjective et on conclut à sa bijectivité. □

Théorème 18. *Soient f et g deux fonctions multiplicatives. Alors la fonction $f * g$ est multiplicative.*

Démonstration. Soient m et n dans $\mathbb{N}^*$ premiers entre eux. On a

$$(f * g)(mn) = \sum_{d \in \mathcal{D}_{mn}} f(d) g\left(\frac{mn}{d}\right)$$

D'après la bijectivité de l'application π de la proposition précédente, il vient

$$(f * g)(mn) = \sum_{(d_1, d_2) \in \mathcal{D}_n \times \mathcal{D}_m} f(d_1 d_2) g\left(\frac{n}{d_1}\frac{m}{d_2}\right)$$

Les entiers m et n étant premiers entre eux, leurs diviseurs respectifs le sont également et par suite

$$\begin{aligned}(f * g)(mn) &= \sum_{(d_1, d_2) \in \mathcal{D}_n \times \mathcal{D}_m} f(d_1) f(d_2) g\left(\frac{n}{d_1}\right) g\left(\frac{m}{d_2}\right) \\ &= \left(\sum_{d_1 | n} f(d_1) g\left(\frac{n}{d_1}\right)\right)\left(\sum_{d_2 | m} f(d_2) g\left(\frac{n}{d_2}\right)\right) = (f * g)(m)(f * g)(n)\end{aligned}$$

□

3 Séries de Dirichlet

Définition 13. *Soit f une fonction arithmétique. On appelle* série de Dirichlet *de la fonction f la série $\sum_{n \geqslant 1} \frac{f(n)}{n^s}$ avec s réel.*

Pour f une fonction arithmétique, on définit son *abscisse de convergence* notée $\mathrm{A}_c(f)$ par

$$\mathrm{A}_c(f) = \inf\left\{ s \in \mathbb{R} \mid \sum_{n \geqslant 1} \frac{f(n)}{n^s} \text{ converge absolument} \right\}$$

avec la convention $\inf \varnothing = +\infty$.

Proposition 14. *Soit f une fonction arithmétique. Si $s > \mathrm{A}_c(f)$, alors la série $\sum_{n \geqslant 1} \frac{f(n)}{n^s}$ converge absolument.*

Démonstration. Soit $s > \mathrm{A}_c(f)$. Par caractérisation de la borne inférieure, on dispose de t tel que $\mathrm{A}_c(f) \leqslant t < s$ et $\sum_{n \geqslant 1} \frac{f(n)}{n^t}$ converge absolument. Or, on a

$$\frac{f(n)}{n^s} \underset{n \to +\infty}{=} \mathrm{o}\left(\frac{f(n)}{n^t}\right)$$

d'où le résultat par comparaison. □

Théorème 19. *Soient f et g des fonctions arithmétiques d'abscisses de convergences finies. On a*

$$\forall s > \max(\mathrm{A}_c(f), \mathrm{A}_c(g)) \qquad \mathrm{L}_{f*g}(s) = \mathrm{L}_f(s)\mathrm{L}_g(s)$$

Démonstration. Soit $s > \max(\mathrm{A}_c(f), \mathrm{A}_c(g))$. Pour $n \in \mathbb{N}^*$, on note $\mathcal{C}_n = \left\{(a,b) \in (\mathbb{N}^*)^2,\ ab = n\right\}$. La famille $(\mathcal{C}_n)_{n\in\mathbb{N}^*}$ constitue une partition de $(\mathbb{N}^*)^2$. D'après le théorème de Fubini, la famille $\left(\dfrac{f(a)}{a^s}\dfrac{g(b)}{b^s}\right)_{(a,b)\in(\mathbb{N}^*)^2}$ est sommable. Par sommation par paquets, il vient

$$\mathrm{L}_f(s)\mathrm{L}_g(s) = \sum_{(a,b)\in(\mathbb{N}^*)^2} \frac{f(a)g(b)}{(ab)^s} = \sum_{n=1}^{+\infty} \frac{1}{n^s} \sum_{(a,b)\in\mathcal{C}_n} f(a)g(b) = \mathrm{L}_{f*g}(s)$$

□

Théorème 20. *Soit f une fonction multiplicative d'abscisse de convergence finie. On a*

$$\forall s > \mathrm{A}_c(f) \qquad \mathrm{L}_f(s) = \prod_{p\in\mathcal{P}} \left(\sum_{k=0}^{+\infty} \frac{f(p^k)}{p^{ks}}\right)$$

Esquisse de preuve. Soit N entier $\geqslant 2$. On note $\{p \in \mathcal{P}, p \leqslant \mathrm{N}\} = \{p_1, \ldots, p_r\}$ avec r qui dépend de N . On peut établir

$$\prod_{p\in\mathcal{P}} \left(\sum_{k=0}^{+\infty} \frac{f(p^k)}{p^{ks}}\right) = \lim_{\mathrm{N}\to+\infty} \prod_{p\in\mathcal{P}, p\leqslant\mathrm{N}} \left(\sum_{k=0}^{+\infty} \frac{f(p^k)}{p^{ks}}\right)$$

Puis

$$\prod_{p\in\mathcal{P}, p\leqslant\mathrm{N}} \left(\sum_{k=0}^{+\infty} \frac{f(p^k)}{p^{ks}}\right) = \sum_{(k_1,\ldots,k_r)\in\mathbb{N}^r} \prod_{i=1}^{r} \frac{f(p_i^{k_i})}{p_i^{k_i s}} = \sum_{(k_1,\ldots,k_r)\in\mathbb{N}^r} \frac{f\left(\prod_{i=1}^{r} p_i^{k_i}\right)}{\left(\prod_{i=1}^{r} p_i^{k_i}\right)^s} = \sum_{n\in\mathcal{N}_\mathrm{N}} \frac{f(n)}{n^s}$$

avec $\mathcal{N}_\mathrm{N}$ les entiers ayant des facteurs premiers $\leqslant$ N. Enfin pour n entier non nul, on peut trouver N assez grand tel que $n \in \mathcal{N}_\mathrm{N}$ et la somme indexée par $\mathcal{N}_\mathrm{N}$ tend vers une somme indexée par $\mathbb{N}$

$$\prod_{p\in\mathcal{P}} \left(\sum_{k=0}^{+\infty} \frac{f(p^k)}{p^{ks}}\right) = \lim_{\mathrm{N}\to+\infty} \sum_{n\in\mathcal{N}_\mathrm{N}} \frac{f(n)}{n^s} = \sum_{n=1}^{+\infty} \frac{f(n)}{n^s}$$

□

Théorème 21. *Soit f une fonction complètement multiplicative d'abscisse de convergence finie. On a*

$$\forall s > \mathrm{A}_c(f) \qquad \mathrm{L}_f(s) = \prod_{p\in\mathcal{P}} \frac{1}{1 - \dfrac{f(p)}{p^s}}$$

Esquisse de preuve. Soient $s > \mathrm{A}_c(f)$ et $p \in \mathcal{P}$. Les termes $\left(\dfrac{f(p)}{p^s}\right)^k = \dfrac{f(p^k)}{(p^k)^s}$ sont issues de la suite $\left(\dfrac{f(n)}{n^s}\right)_{n\geqslant 1}$ d'où la convergence absolue de $\sum \left(\dfrac{f(p)}{p^s}\right)^k$ puis

$$\frac{1}{1 - \dfrac{f(p)}{p^s}} = \sum_{k=0}^{+\infty} \left(\frac{f(p)}{p^s}\right)^k$$

On conclut avec l'égalité du théorème précédent.

□

Annexe

Théorème 5. *Soit n entier avec $n \geqslant 2$. Alors, on a $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec r entier non nul, les p_i des nombres premiers deux à deux distincts et les α_i des entiers non nuls. Cette décomposition est unique à l'ordre près.*

Démonstration. Pour l'existence, on procède par récurrence forte sur n. Le cas $n = 2$ est immédiat. Supposons le résultat vrai jusqu'à l'entier $n \geqslant 2$ fixé. Si $n+1$ est premier, on a le résultat. Sinon, l'entier $n+1$ admet un diviseur strict premier p et notant $n+1 = pk$ avec $k \geqslant 2$, on applique l'hypothèse de récurrence à l'entier k. L'existence suit par principe de récurrence. Supposons qu'on dispose de deux décompositions de $n \geqslant 2$

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{j=1}^{s} q_j^{\beta_j}$$

avec r, s entiers non nuls, les p_i et q_j des nombres premiers deux à deux distincts et les α_i et β_j entiers non nuls. Soit $i \in [\![1\,;\, r]\!]$. On a $p_i | \prod_{j=1}^{s} q_j^{\beta_j}$ d'où, d'après le lemme d'Euclide, l'existence de $j \in [\![1\,;\, s]\!]$ tel que $p_i | q_j^{\beta_j}$ et d'où $p_i | q_j$ par primalité de p_i. Comme q_j est également premier, il s'ensuit $p_i = q_j$. L'indice j correspondant à i est unique puisque les nombres premiers q_j intervenant dans la décomposition sont deux à deux distincts. Ainsi, pour $i \in [\![1\,;\, r]\!]$, il existe un unique $j \in [\![1\,;\, s]\!]$ tel que $p_i = q_j$ On dispose d'une injection de $[\![1\,;\, r]\!]$ dans $[\![1\,;\, s]\!]$ d'où $r \leqslant s$ et par symétrie des rôles, on trouve $r = s$. Les facteurs premiers intervenant dans chacune des décompositions sont donc les mêmes et en même nombre. Enfin, pour $i \in [\![1\,;\, r]\!]$ et $j \in [\![1\,;\, r]\!] \setminus \{i\}$, on a $p_i \wedge p_j = 1$ d'où $p_i^{\alpha_i} \wedge p_j^{\beta_j} = 1$ puis

$$p_i^{\alpha_i} \wedge \prod_{j \in [\![1\,;\, r]\!] \setminus \{i\}} p_j^{\beta_j} = 1$$

D'après le lemme de Gauss, il s'ensuit $p_i^{\alpha_i} | p_i^{\beta_i}$ d'où $\alpha_i \leqslant \beta_i$ puis $\alpha_i = \beta_i$ par symétrie des rôles ce qui clôt l'unicité. □