Chapitre XI : Arithmétiques

Retranscrit par Samy Youssoufine

11 février 2026

Note importante

Peut contenir des erreurs ou des sections incomplètes.

Table des matières

Ce chapitre est consacré à l'arithmétique dans un anneau intègre (cas général). On étudiera ensuite des cas particuliers de cette dernière.

1 Divisibilité dans un anneau intègre

1.1 Divisibilité et éléments associés

Définition 1.1.1.1

Soient A un anneau intègre (commutatif) et x, y des éléments de A. On dit que x divise y dans A lorsqu'il existe un $a \in A$ tel que $y = xa = ax$ (sachant que la multiplication est commutative). On note alors $x \mid y$ (**pas** noté x/y !).

Exemple 1.1.1.1

Prenons $A = \mathbb{Z}[i]$ l'anneau des entiers gaussiens. Cet anneau est intègre parce que c'est un sous-anneau de $\mathbb{C}$, qui est intègre, parce que $\mathbb{C}$ est un corps.
On cherche les diviseurs de 2 dans $\mathbb{Z}[i]$. On remarque que $2 = (1+i)(1-i)$, donc $1+i$ et $1-i$ divisent 2. On peut aussi remarquer que $2 = (-i)(-2i)$, donc $-2i$ divise aussi 2.
Nous allons maintenant rechercher tous les diviseurs de 2 dans $\mathbb{Z}[i]$.
Soit $x = a + ib \in \mathbb{Z}[i]$ un diviseur de 2. Alors il existe un $y = c + id$ tel que $xy = 2 \iff (a+ib)(c+id) = 2$.
On utilise le module pour trouver des contraintes sur a et b :

$$\underbrace{(a^2+b^2)}_{\in\mathbb{N}}\underbrace{(c^2+d^2)}_{\in\mathbb{N}} = |xy|^2 = |2|^2 = 4.$$

Cela implique que a^2+b^2 divise 4 dans $\mathbb{N}$. Cela implique que $a^2+b^2 \in \{1, 2, 4\}$ (car a^2+b^2 est une somme de carrés d'entiers).

- Si $a^2 + b^2 = 1$, alors $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$. Cela donne les diviseurs $1, -1, i, -i$.
- Si $a^2+b^2 = 2$, alors $(a, b) \in \{(\pm 1, \pm 1)\}$. Cela donne les diviseurs $1+i, 1-i, -1+i, -1-i$.
- Si $a^2 + b^2 = 4$, alors $(a, b) \in \{(\pm 2, 0), (0, \pm 2)\}$. Cela donne les diviseurs $2, -2, 2i, -2i$.

La réciproque est facile à vérifier. Ainsi, les diviseurs de 2 dans $\mathbb{Z}[i]$ sont :

$$\{\pm 1, \pm i, \pm(1+i), \pm(1-i), \pm 2, \pm 2i\}.$$

Dans la suite de cette partie, toute mention de $(A, +, \times)$ désignera un anneau intègre commutatif.

Propriété 1.1.1.1

1. Pour tout $x \in A$, on a $x \mid x$ (réflexivité).
2. Pour tout $x, y, z \in A$, si $x \mid y$ et $y \mid z$, alors $x \mid z$ (transitivité).
3. Pour tout $x, y \in A$, $x \mid y \iff yA \subset xA$. Il faut faire attention à ne pas inverser les deux membres ! Cette relation nous permet de passer de la relation de divisibilité à une inclusion (inégalité).
4. Pour tout $x, y \in A, (x \mid y \text{ et } y \mid x) \iff xA = yA$. Cela équivaut à dire que $\exists \varepsilon \in \mathbb{U}_A$ tel que $x = \varepsilon y$. On dit que x et y sont **associés** dans ce cas.
5. La relation de divisibilité n'est pas antisymétrique. Par exemple, dans $\mathbb{Z}$, $2 \mid -2$ et $-2 \mid 2$, mais $2 \neq -2$.
6. La relation de divisibilité n'est pas symétrique, par exemple dans $\mathbb{Z}$, $2 \mid 4$, mais $4 \nmid 2$.
7. La relation de divisibilité n'est donc pas une relation d'équivalence.

Preuve

1. Trivial car $x = x \cdot 1_A$.
2. $(x \mid y)$ et $(y \mid z)$ impliquent l'existence de $a, b \in A$ tels que $y = xa$ et $z = yb$. Donc $z = (xa)b = x(ab)$, donc $x \mid z$.
3. ($\Longleftarrow$) : On a $y = y \cdot 1_A \in yA \subset xA$, donc $y \in xA \iff \exists a \in A$ tel que $y = ax$, donc $x \mid y$.
   ($\Longrightarrow$) : Supposons que $x \mid y$, alors $\exists a \in A$ tel que $y = ax$. Soit $t \in yA$, i.e. $\exists \alpha \in A$ tel que $t = y\alpha$.
   Donc $t = (ax)\alpha = x\underbrace{(a\alpha)}_{\in A} \in xA$. Ainsi, $yA \subset xA$.
4. D'après la propriété précédente, $x \mid y$ et $y \mid x$ équivaut à $yA \subset xA$ et $xA \subset yA$, donc $xA = yA$.
   Maintenant, nous allons montrer que $(x \mid y \text{ et } y \mid x) \iff \exists \varepsilon \in \mathbb{U}_n$ tel que $x = \varepsilon y$.
   Dans le sens réciproque, on a $x = \varepsilon y \implies y \mid x$, or $\varepsilon \in \mathbb{U}_A \implies \exists \varepsilon' \in \mathbb{U}_A$ tel que $\varepsilon' x = y$. D'où $x \mid y$.
   Dans le sens direct, on suppose que $x \mid y$ et $y \mid x$. Donc il existe $t, z \in A$ tel que $y = tx$ et $x = zy$.
   Donc $y = t(zy) = (tz)y$. Donc $y(1_A - tz) = 0_A$. Comme A est intègre, cela veut dire que $y = 0_A$ ou $1_A - tz = 0_A \iff tz = 1_A$. Dans le deuxième cas, cela veut dire que $tz = 1_A$, donc $z = \varepsilon \in \mathbb{U}_A$, et on a bien $x = zy = \varepsilon y$. Dans le premier cas, on a $y = 0_A$, donc $x = zy = z0_A = 0_A$. On peut alors choisir $\varepsilon = 1_A \in \mathbb{U}_A$ et on a bien $x = \varepsilon y$.
   Ainsi, dans tous les cas, on a $\exists \varepsilon \in \mathbb{U}_A$ tel que $x = \varepsilon y$.

■

Exemple 1.1.1.2

1. $\mathbb{U}_{\mathbb{Z}} = \{-1, 1\}$. Donc, dans $\mathbb{Z}$, $(x \mid y \text{ et } y \mid x) \iff \exists \varepsilon \in \{-1, 1\}$ tel que $x = \varepsilon y$. Cela équivaut à dire que $x = \pm y$, ou que $|x| = |y|$.
2. Dans $\mathbb{Z}[i]$, on a $\mathbb{U}_{\mathbb{Z}[i]} = \{1, -1, i, -i\}$. Donc, dans $\mathbb{Z}[i]$, $(x \mid y \text{ et } y \mid x) \iff \exists \varepsilon \in \{1, -1, i, -i\}$ tel que $x = \varepsilon y$.

1.2 Idéaux/anneaux principaux et PGCD

Définition 1.1.2.2 ***(Anneau principal)***

1. Soit I un idéal de A, I est un **idéal principal** de A lorsque I est engendré par un seul élément x de A. i.e. I est un idéal principal $\iff \exists x \in A$ tel que $I = xA$.
2. Un anneau A est dit principal lorsque tout les idéaux sont principaux. i.e. $\forall I$ idéal de $A, \exists x \in A$ tel que $I = xA$.

Attention

Un anneau principal n'est pas forcément un anneau intègre. Par exemple, $\mathbb{Z}/6\mathbb{Z}$ est un anneau principal (voir exemple plus bas), mais ce n'est pas un anneau intègre car $\overline{2} \times \overline{3} = \overline{0}$ dans $\mathbb{Z}/6\mathbb{Z}$.

Exemple 1.1.2.3

1. $\mathbb{Z}$ est un anneau principal.
2. Tout corps est un anneau principal parce que les seuls idéaux sont $\{0\}$ et le corps lui-même, qui sont tous deux principaux.
3. On a déjà vu que les idéaux de $\mathbb{Z}/4\mathbb{Z}$ sont $\{0\}, 2\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$, qui sont tous des idéaux principaux. Donc $\mathbb{Z}/4\mathbb{Z}$ est un anneau principal.

Exercice 1.1.2.1

Montrer que $\mathbb{Z}/6\mathbb{Z}$ est un anneau principal.

Théorème 1.1.2.1 *(PGCD dans un anneau principal)*

Soient A un anneau principal et $x_1, \dots, x_n \in A$. Alors il existe un $d \in A$ tel que :

$$x_1A + x_2A + \cdots + x_nA = dA$$

avec $\forall i \in [\![1, n]\!], d \mid x_i$.
De plus, si d' est un autre élément de A vérifiant ces propriétés, alors $d' \mid d$.
Dans cas, d est appelé le **plus grand commun diviseur** (PGCD) des x_i.
On le note $\text{pgcd}(x_1, \dots, x_n)$.

Preuve

- On a $\forall i \in [\![1, n]\!], x_iA$ est un idéal principal.
- Donc $\sum_{i=1}^n x_iA = x_1A + \cdots + x_nA$ est aussi un idéal de A, qui est principal, puisque l'anneau A est principal.
- Donc $\exists d \in A$ tel que $\sum_{i=1}^n x_iA = dA$.
- On a $\forall i \in [\![1, n]\!], x_i = x_i \times 1_A + \sum_{j=1 \text{ et } j\neq i}^n x_j \times 0_A \in \sum_{i=1}^n x_iA = dA$.
- Donc $\forall i \in [\![1, n]\!], d \mid x_i$.
- Si $d' \in A$ tel que $\forall i \in [\![1, n]\!], d' \mid x_i$.
- Alors $\forall i \in [\![1, n]\!], x_iA \subset d'A$.
- Comme dA est stable par l'addition (sous-groupe), alors $dA = \sum_{i=1}^n x_iA \subset d'A \implies d'|d$.

■

Remarque 1.1.2.1 *(Non unicité du PGCD)*

Si d est un PGCD de x_i, alors tout autre PGCD d' est associé à d. En effet, on a $d' \mid d$ et $d \mid d'$. Ils peuvent s'écrire sous la forme de $d' = \varepsilon d$ avec $\varepsilon \in \mathbb{U}_A$.

Remarque 1.1.2.2

$\mathbb{Z}$ est un anneau principal, donc $\forall x_1, \dots, x_n \in \mathbb{Z}, \exists d \in \mathbb{Z}$ tel que $x_1\mathbb{Z} + \cdots + x_n\mathbb{Z} = d\mathbb{Z}$. Or, tous les pgcd des $(x_i)_{1\leq i\leq n}$ sont $\pm d$.
Alors, $\forall x_1, \dots, x_n \in \mathbb{Z}, \exists! d \in \mathbb{N}$ tel que $\sum_{i=1}^n x_i\mathbb{Z} = d\mathbb{Z}$.
Dans ce cas, d est appelé le PGCD des x_i dans $\mathbb{Z}$.

Théorème 1.1.2.2 *(Égalité de Bézout)*

Soient A un anneau principal et $x_1, \dots, x_n \in A$. Alors, si d est un $\text{pgcd}(x_1, \dots, x_n)$, alors :

$$\exists u_1, \dots, u_n \in A \text{ tel que } d = u_1x_1 + u_2x_2 + \cdots + u_nx_n.$$

Preuve

On a $\sum_{i=1}^{n} x_i A = dA$. Donc, $d \in dA = \sum_{i=1}^{n} x_i A$. ■

Propriété 1.1.2.2 *(Réciproque de l'égalité de Bézout)*

Soient $x_1, \ldots, x_n \in A$ (anneau principal), et d un élément de A tel que $\exists u_1, \ldots, u_n \in A$ tel que $d = u_1 x_1 + u_2 x_2 + \cdots + u_n x_n$.
d n'est pas forcément le PGCD des x_i. Il faut que d soit un diviseur commun des x_i pour que d soit le PGCD des x_i.

Preuve

Montrons que $\sum_{i=1}^{n} x_i A = dA$.
Montrons d'abord l'inclusion $\sum_{i=1}^{n} x_i A \subset dA$.
Soit $y \in dA$. DOnc $y = da$ pour un certain $a \in A$.
Donc $y = (\sum_{i=1}^{n} x_i u_i)a = \sum_{i=1}^{n} x_i \underbrace{(u_i a)}_{\in A}$
Donc $y \in \sum_{i=1}^{n} x_i A$.
i.e. : $dA \subset \sum_{i=1}^{n} x_i A$.
On conclut que $\sum_{i=1}^{n} x_i A = dA$.
D'où $d = \text{pgcd}(x_1, \ldots, x_n)$. ■

Conséquence 1.1.2.1 *(Théorème de Bézout pour le PGCD)*

Soient $x_1, \ldots, x_n \in A$ principal.
$\text{pgcd}(x_1, \ldots, x_n) = 1_A \iff \exists u_1, \ldots, u_n \in A$ tel que $\sum_{i=1}^{n} x_i u_i = 1_A$.
On dit que les x_i sont **premiers entre eux** dans ce cas.

Théorème 1.1.2.3 *(Théorème de Gauss)*

Soient A un anneau principal et $x, y, z \in A$ tels que $x \mid yz$ et $\text{pgcd}(x, z) = 1_A$. Alors $x \mid y$.

Preuve

On a $x \mid yz$, donc $\exists a \in A$ tel que $yz = xa$.
On sait aussi que $\text{pgcd}(x, z) = 1_A$, cela équivaut à dire que $\exists u_1, u_2 \in A$ tel que $1_A = u_1 x + u_2 z$.
Donc $y = xyu_1 + yzu_2$.
Donc $y = xyu_1 + (xa)zu_2 = x \underbrace{(yu_1 + au_2 z)}_{\in A}$.
Donc $x \mid y$. ■

Conséquence 1.1.2.2

Soient $y_1, \dots, y_n$ et $x_1, \dots, x_n$ des éléments de A.
On a :

$$(\forall i, j \in [\![1, n]\!], \text{pgcd}(x_i, x_j) = 1_A) \iff \left(\prod_{i=1}^{n} x_i\right) \wedge \left(\prod_{i=1}^{n} y_i\right) = 1_A$$

Propriété 1.1.2.3

Soient $x, y, z \in A$ (anneau principal).

$$(x \wedge y = x \wedge z = 1_A) \iff x \wedge (yz) = 1_A$$

Preuve

1. ($\Longleftarrow$) : Facile.
2. ($\Longrightarrow$) : On a $\exists u_1, u_2, v_1, v_2 \in A$ tel que $\begin{cases} xu_1 + yu_2 = 1_A \\ xv_1 + zv_2 = 1_A \end{cases}$
3. Cela implique que $x(\underbrace{xu_1v_1 + zu_1v_2 + yu_2v_1}_{\in A}) + yz(u_2v_2) = 1_A$.
4. Donc $x \wedge (yz) = 1_A$.

■

Preuve *(Démonstration de la conséquence 2)*

En utilisant la propriété précédente, on peut

■ recop

Application 1.1.2.1

Montrer que $\sqrt[3]{2}$ n'appartient pas à $\mathbb{Q}$.
Solution :
Supposons que $\sqrt[3]{2} \in \mathbb{Q}$.
Alors, il existe $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $\sqrt[3]{2} = \frac{p}{q}$ et $\text{pgcd}(p, q) = 1$.
On a donc $2q^3 = p^3$.
Donc $q^3 \mid p^3$.
Donc $\text{pgcd}(p^3, q^3) = 1$ (car $\text{pgcd}(p, q) = 1$).
Or, comme $q^3 \mid p^3$ et $\text{pgcd}(p^3, q^3) = 1$, d'après le théorème de Gauss, on a $q^3 \mid 1$, donc $q = 1$.
Donc $p^3 = 2$.
Or $1 < 2 < 8 = 2^3$, donc $1^3 < p^3 < 2^3$, donc $1 < p < 2$, ce qui est impossible.
Donc $\sqrt[3]{2} \notin \mathbb{Q}$.

Propriété 1.1.2.4

Soient A un anneau principal et x, y, z dans A.
Si $x \mid y$ et $y \mid z$ avec $\text{pgcd}(x, y) = 1_A$, alors $xy \mid z$.

Preuve

On sait que $\exists a, b \in A$ tels que $z = xa$ et $z = yb$.
Donc $\exists u, v \in A$ tels que $xu + yv = 1_A$.

$$\begin{aligned} \implies z &= z(xu + yv) \\ &= xybu + xyav = xy(bu + av) \\ &impliesxy \mid z. \end{aligned}$$

■

Conséquence 1.1.2.3

Si $x_1, \ldots, x_n, z \in A$ (avec A un anneau principal). On a :

$$\begin{cases} \forall i \in [\![1, n]\!], x_i \mid z \\ \forall i, j \in [\![1, n]\!], \text{pgcd}(x_i, x_j) = 1_A \end{cases} \implies \prod_{i=1}^{n} x_i \mid z$$

Preuve

On procède par récurrence sur n. ■

Remarque 1.1.2.3

En général, $\begin{cases} x \mid z \\ y \mid z \end{cases} \not\implies xy \mid z.$
(On prend comme contre-exemple $4 \mid 12$ et $6 \mid 12$...)

Propriété 1.1.2.5

Soient $t, x, y \in \mathbb{Z}$.
On a $(tx) \wedge (ty) = |t|(x \wedge y)$.

Preuve

On pose $d = (tx) \wedge (ty)$.
On a alors $(tx)\mathbb{Z} + (ty)\mathbb{Z} = d\mathbb{Z}$ (définition du PGCD dans $\mathbb{Z}$).
Ce qui implique que $t(x\mathbb{Z} + y\mathbb{Z}) = d\mathbb{Z}$ (opérations sur les ensembles).

Donc $t(x \wedge y)\mathbb{Z} = d\mathbb{Z}$.
Donc $|t(x \wedge y)| = d$ (car ces deux entiers sont associés, voir propriété 1).
Donc $d = |t|(x \wedge y)$. ■

Propriété 1.1.2.6

Soient A un anneau principal et $x, y \in A$.

$$x \wedge y = d \iff \exists x_1, y_1 \in A \text{ tel que } \begin{cases} x = dx_1 \\ y = dy_1 \\ x_1 \wedge y_1 = 1_A \end{cases}$$

Preuve

Dans le sens direct ($\Longrightarrow$), on suppose que $d \mid x$ et $d \mid y$.
Donc $\exists x_1, y_1 \in A$ tel que $x = dx_1$ et $y = dy_1$.
Or $x \wedge y = d = (dx_1) \wedge (dy_1)$
Donc $d = d(x_1 \wedge y_1)$.
Alors $d(1_A - (x_1 \wedge y_1)) = 0_A$.
Si $d = 0_A$, alors $x = y = 0_A$, donc on peut choisir $x_1 = y_1 = 1_A$ et on a bien $x_1 \wedge y_1 = 1_A$.
Si $d \neq 0_A$, comme A est intègre, on a $1_A - (x_1 \wedge y_1) = 0_A$, donc $x_1 \wedge y_1 = 1_A$.
Dans le sens réciproque ($\Longleftarrow$), on a $x = dx_1$ et $y = dy_1$.
On sait que $x_1 \wedge y_1 = 1_A$.
Donc $\exists u, v \in A$ tel que $1_A = ux_1 + vy_1$.
Donc $d = d(ux_1 + vy_1) = u(dx_1) + v(dy_1) = ux + vy$.
Donc $x \wedge y = d$. ■

2 Divisibilité dans $\mathbb{Z}/n\mathbb{Z}$

2.1 Rappels et compléments sur $\mathbb{Z}/n\mathbb{Z}$

Remarque 2.2.1.4

1. Soient $x, y \in \mathbb{Z}^*$ tels que $x \mid y$. On a donc $-x \mid y$, on prendra donc toujours $x \in \mathbb{N}^*$ sans perte de généralité. Donc $x \mid y \iff \overline{y} = \overline{0}$ dans $\mathbb{Z}/x\mathbb{Z}$.
2. $\mathbb{U}_{\mathbb{Z}/n\mathbb{Z}} = \{\overline{x} \text{ tel que } x \wedge n = 1\}$.
   On rappelle le théorème de Gauss dans $\mathbb{Z}$: $(x \mid yz \text{ et } x \wedge y = 1) \implies x \mid z$.

Preuve

On a $x \mid yz \iff \overline{y \cdot z} = \overline{0}$ dans $\mathbb{Z}/|x|\mathbb{Z}$.

$$\begin{aligned} \text{On a } x \wedge y = 1 &\iff \overline{y} \in \mathbb{U}_{\mathbb{Z}/|x|\mathbb{Z}} \\ \text{Hypothèse de départ} &\implies \overline{y} \cdot \overline{z} = \overline{0} \text{ dans } \mathbb{Z}/|x|\mathbb{Z} \\ &\implies \overline{y}^{-1} \cdot \overline{y} \cdot \overline{z} = \overline{y}^{-1} \cdot \overline{0} \\ &\qquad \overline{z} = \overline{0} \text{ dans } \mathbb{Z}/|x|\mathbb{Z} \\ &\implies x \mid z. \end{aligned}$$

■

Exercice 2.2.1.2

1. Montrer que $\forall n \in \mathbb{N}, 6 \mid n^3 - n$.
2. Pour quelles valeurs de $n \in \mathbb{N}$ a-t-on $11 \mid n^3 + n$?

Solution :

1. On peut tout simplement démontrer qu'il s'agit d'un produit de trois nombres consécutifs, dont un est forcément pair. Mais on peut aussi faire ce calcul :
   $C_3^{n+1} = \cdots = \frac{(n-1)n(n+1)}{6} \in \mathbb{N}$.
   Donc $6 \mid n^3 - n$.
2. $11 \mid n^3 + n \iff \overline{n}(\overline{n^2 + 1}) = \overline{0}$ dans $\mathbb{Z}/11\mathbb{Z}$.

On dresse un tableau des carrés dans $\mathbb{Z}/11\mathbb{Z}$. On trouve que $11 \mid n^3+n$ lorsquee $\overline{n}(\overline{n^2+1}) = \overline{0}$. C'est-à-dire lorsque $\overline{n} = \overline{0}$ dans $\mathbb{Z}/11\mathbb{Z}$ (le cas $\overline{n^2+1} = \overline{0}$ n'ayant pas de solution). Donc $11 \mid n^3+n \iff 11 \mid n$.

Propriété 2.2.1.7 *(Divisibilité par 3)*

Soit $x = a_n \dots a_0$ l'écriture en base décimale de $x \in \mathbb{N}$.

$$3 \mid x \iff 3 \mid \sum_{k=0}^{n} a_k$$

Preuve

On a $x = \sum_{k=0}^{n} a_k \cdot 10^k$.

$$\begin{aligned}
\text{On a } 3 \mid x &\iff \overline{x} = \overline{0} \text{ dans } \mathbb{Z}/3\mathbb{Z} \\
&\iff \sum_{k=0}^{n} \overline{a_k \cdot 10^k} = \overline{0} = \overline{\sum_{k=0}^{n} a_k} \text{ dans } \mathbb{Z}/3\mathbb{Z} \\
&\iff \sum_{k=0}^{n} \overline{a_k} = \overline{0} \text{ dans } \mathbb{Z}/3\mathbb{Z} \\
&\iff 3 \mid \sum_{k=0}^{n} a_k
\end{aligned}$$

■

2.2 Division euclidienne et algorithme d'Euclide

Théorème 2.2.2.4 *(Division euclidienne)*

Soient $(x, y) \in \mathbb{Z} \times \mathbb{Z}^*$.

Alors $\exists!(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que : $\begin{cases} x = qy + r \\ 0 \leq r < |y| \end{cases}$

On dit qu'on a effectué la division euclidienne (qu'on notera D.E.) de x par y.

- q est appelé le **quotient** de la D.E. de x par y.
- r est appelé le **reste** de la D.E. de x par y.

Preuve

$$\begin{cases} x = qy + r \\ 0 \leq r < |y| \end{cases} \iff \begin{cases} r = x - qy \\ 0 \leq x - qy < |y| \end{cases}$$
$$\iff \begin{cases} r = x - qy \\ 0 \leq \frac{x}{|y|} - q\frac{y}{|y|} < 1 \end{cases}$$

Si $y > 0$, alors on a $\begin{cases} r = x - qy \\ 0 \leq \frac{x}{y} - q < 1 \end{cases}$
On prend $q = E(\frac{x}{y}) \in \mathbb{Z}$, et $r = x - qy \in \mathbb{N}^*$.
Si $y < 0$, alors on a $\begin{cases} r = x - qy \\ -q \leq -\frac{x}{y} < 1 - q \end{cases}$
Donc on prend $q = -E(-\frac{x}{y}) \in \mathbb{Z}$, et $r = x - qy \in \mathbb{N}^*$.
D'où l'existence et l'unicité de (q, r). ■

Propriété 2.2.2.8

Soient $(x, y) \in \mathbb{Z} \times \mathbb{Z}^*$.
On a $\exists!(q, r) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $\begin{cases} x = qy + r \\ 0 < r \leq |y| \end{cases}$
Le PGCD de x et y est égal au PGCD de y et r.

$$x \wedge y = y \wedge r$$

Preuve

On pose $d = x \wedge y$, et $d' = y \wedge r$.
Méthode 1 (plus facile) en utilisant les combinaisons linéaires : (non abordée).
Méthode 2 en utilisant la définition du PGCD :

$$\begin{aligned} d\mathbb{Z} &= x\mathbb{Z} + y\mathbb{Z} \\ &= (qy + r)\mathbb{Z} + y\mathbb{Z} \\ &\subset r\mathbb{Z} + y\mathbb{Z} = d'\mathbb{Z} \end{aligned}$$

De même, $d'\mathbb{Z} = y\mathbb{Z} + r\mathbb{Z} \subset x\mathbb{Z} + y\mathbb{Z} = d\mathbb{Z}$.
Donc $|d| = |d'| \implies d = d'$ car ils sont positifs.
On en déduit que $x \wedge y = y \wedge r$.

■

Application 2.2.2.2 ***(Algorithme d'Euclide)***

Cet algorithme nous permet de déterminer le PGCD de deux entiers a et b ainsi que leurs coefficients de Bézout.
Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$.

- Si $b \mid a$ alors $a \wedge b = b$.
- Sinon, $a = bq + r_1$ avec $0 < r_1 < b$ (après division euclidienne).
- Donc $a \wedge b = b \wedge r_1$.
- Si $r_1 \mid b$ alors $a \wedge b = r_1$.
- Sinon, $b = r_1 q_2 + r_2$ avec $0 < r_2 < r_1$.
- Donc $a \wedge b = r_1 \wedge r_2$.
- On continue ainsi jusqu'à obtenir un reste r_n qui divise le précédent.

On a donc construit une suite de restes $(r_n)_{n\geq 1}$. Ce processus doit s'arrêter car les restes sont strictement décroissants et positifs. Si le processus ne s'arrête pas, on aurait une suite infinie de restes strictement positifs et décroissants, ce qui est impossible dans $\mathbb{N}$, car la suite doit être stationnaire à partir d'un certain rang.
Le dernier reste non nul r_n est le PGCD de a et b.

Exemple 2.2.2.4

Calculer le PGCD de $a = 60$ et $b = 42$.
On a $a = 60 = 1 \times 42 + 18$. Et on a $b = 42 = 2 \times 18 + 6$. Enfin, on a $18 = 3 \times 6 + 0$.
Donc le PGCD de 60 et 42 est 6.
Nous allons retrouver les coefficients de Bézout associés.
On a $6 = 42 - 2 \times 18$.
Or, $18 = 60 - 1 \times 42$.
Donc $6 = 42 - 2 \times (60 - 1 \times 42) = 3 \times 42 - 2 \times 60$.
Ainsi, les coefficients de Bézout sont $u = -2$ et $v = 3$.

Propriété 2.2.2.9 ***(Équation $ax + by = c$)***

Soient A un anneau principal et $a, b, c \in A$ tel que $(a, b) \neq (0_A, 0_A)$.
On pose $d = a \wedge b$.
Les solutions de l'équation $ax + by = c$ sont données par :

$$\begin{cases} \text{si } d \nmid c, \text{ il n'y a pas de solution} \\ \text{si } d \mid c, \exists \text{ une solution } (x_0, y_0) \text{ et } S = \{(x, y) = (x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k) \text{ avec } k \in A\} \end{cases}$$

Preuve

$$a \wedge b = d \iff \exists a_1, b_1 \in A \text{ tels que } a = da_1 \text{ et } b = db_1 \text{ et } a_1 \wedge b_1 = 1_A$$

Donc $(E) : d(a_1x + b_1y) = c$.
Dans le cas où $d \nmid c$, il n'y a pas de solution.
Dans le cas contraire, on a $c = dc_1$ avec $c_1 \in A$.
On va donc trouver l'équation $(E) : a_1x + b_1y = c_1$, sachant que l'anneau A est intègre (donc on peut factoriser par d, puis omettre le cas où $d = 0$, parce que d est un élément non nul).
Comme $a_1 \wedge b_1 = 1_A$, il existe un certain couple (u, v) tels que $a_1u + b_1v = 1_A$.
En multipliant par c_1, on a $a_1(c_1u) + b_1(c_1v) = c_1$.
Donc $(x_0, y_0) = (c_1u, c_1v)$ est une solution particulière de (E).
Soit (x, y) une autre solution de (E).
On obtient le système suivant :

$$\begin{cases} a_1x + b_1y = c_1 \\ a_1x_0 + b_1y_0 = c_1 \end{cases} \implies a_1(x - x_0) = b_1(y - y_0)$$

(Attention : à partir de ce stade, on ne travaille que par implications...)

Cela implique que $b_1 \mid a_1(x - x_0)$.
Cela implique que $b_1 \mid (x - x_0)$ car $a_1 \wedge b_1 = 1_A$ (théorème de Gauss).
Donc $\exists k \in A$ tel que $x - x_0 = b_1k$.
Donc $\exists k \in A$ tel que $x = x_0 + b_1k$.
En remplaçant dans l'équation $a_1(x - x_0) = b_1(y - y_0)$, on obtient :

$$\begin{aligned} & a_1(b_1k) = b_1(y - y_0) \\ \implies & a_1k = y - y_0 \text{ sachant que } b_1 \neq 0 \text{ et } A \text{ est un anneau intègre} \\ \implies & y = y_0 + a_1k \end{aligned}$$

On trouve ensuite que toutes les solutions de l'équation (E) sont de la forme :

$$(x, y) = (x_0 + b_1k, y_0 - a_1k) \text{ avec } k \in A$$

Maintenant, on doit procéder dans le sens réciproque (il ne faut pas oublier qu'on a procédé par implications).
On a $a(x_0+b_1k)+b(y_0-a_1k) = d(a_1uc_1+a_1b_1k+b_1vc_1-b_1a_1k) = d(a_1uc_1+b_1vc_1) = dc_1 = c$.
On conclut que toutes les solutions de l'équation (E) sont de la forme (dans le cas où $d \mid c$) :

$$S = \{(x, y) = (x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k) \text{ tel que } k \in A\}$$

Où (x_0, y_0) est une solution particulière de l'équation $ax + by = c$.
Évidemment, la notation $\frac{a}{d}$ et $\frac{b}{d}$ est valide car $d \mid a$ et $d \mid b$, mais elle n'est pas rigoureuse. Pour être rigoureux, il faudrait écrire a_1 et b_1 à la place de $\frac{a}{d}$ et $\frac{b}{d}$, en mentionnant le fait qu'ils existent etc...

■

Exemple 2.2.2.5

Résolvons dans $\mathbb{Z}^2$ l'équation $(E) : 17x + 7y = 1$.
On a $17 \wedge 7 = 1$.
avec l'algorithme d'Euclide, on trouve :
$17 \times (-2) + 7 \times 5 = 1$.
Donc une solution particulière est $(x_0, y_0) = (-2, 5)$.
On peut donc écrire :

$$\begin{cases} 17x + 7y = 1 \\ 17x - 2 + 7 \times 5 = 1 \end{cases} \implies 17(x+2) = 7(5-y)$$

Comme $7 \wedge 17 = 1$, on a $7 \mid (x+2) \implies \exists k \in \mathbb{Z}$ tel que $x+2 = 7k \implies x = -2+7k$.
Cela implique que $17 \times 7k = 7(5-y) \implies 17k = 5 - y \implies y = 5 - 17k$.
Réciproquement, on vérifie que $17(-2+7k) + 7(5-17k) = 1$.
Donc l'ensemble des solutions de l'équation (E) est :

$$S = \{(x, y) = (-2 + 7k, 5 - 17k) \text{ tel que } k \in \mathbb{Z}\}$$

3 Nombres premiers

3.1 Définition et propriétés

Définition 3.3.1.3 *(Nombre premier)*

Soit $p \in \mathbb{N}^* \setminus \{1\}$.
p est dit **nombre premier** si ses seuls diviseurs sont 1 et p.
On notera par $\mathcal{P}$ l'ensemble des nombres premiers.

Théorème 3.3.1.5 *(Lemme)*

$\forall a \in \mathbb{N}^* \setminus \{1\}, \exists p \in \mathcal{P}$ tel que $p \mid a$.

Preuve

On pose $E = \{k \in \mathbb{N}^* \setminus \{1\}$ tel que $\forall p \in \mathcal{P}, k \mid a\}$.
On a $q \in E \implies E \neq \emptyset$.
Donc $E \subset \mathbb{N}^*$.
Alors E admet un minimum p.
Supposons que p ne soit pas premier. On aura alors :
$\exists 1 < q < p$ tel que $q \mid p$. Or $p \mid a$, alors :
$q \mid a$ et $q \in \mathbb{N}^* \setminus \{1\} \implies q \in E$.
Ce qui implique que $q \geq \min(E) = p$. Contradiction.
DOnc p est premier et divise a.

■

Propriété 3.3.1.10 *(Infinité des nombres premiers)*

Il existe une infinité de nombres premiers. L'ensemble $\mathcal{P}$ est infini.

Preuve

Supposons que $\mathcal{P}$ soit fini, et notons-le $\mathcal{P} = \{p_1, \ldots, p_r\}$, avec chaque p_i deux à deux distincts.
On pose $a = 1 + \prod_{k=1}^{r} p_k > p_i \forall i \in \{1, \ldots, r\}$.

Donc $\begin{cases} a \notin \mathcal{P} \\ a > 1 \end{cases}$ et $\exists j \in \{1, \dots, r\}$ tel que $p_j \mid a$.
Or $\forall j \in \{1, \dots, r\}, p_j \wedge a = 1$, ce qui implique que $p_j 1$ car $p_j \mid a$. C'est une contradiction.
Donc $\mathcal{P}$ est infini. ■

Remarque 3.3.1.5

1. $\forall p \in \mathcal{P}, \forall x \in \mathbb{Z}, p \wedge x = \begin{cases} p & \text{si } p \mid x \\ 1 & \text{sinon} \end{cases}$, i.e. : Soit $p \mid x$, soit p et x sont premiers entre eux.
2. Soient $p \in \mathcal{P}$. On a alors $\forall k \in \{1, \dots, p-1\}, p \mid \mathrm{C}_k^p$.

Preuve

Preuve du deuxième point :
On a $\mathrm{C}_k^p = \frac{p!}{k!(p-k)!}$.
Donc $\mathrm{C}_k^p = \frac{p}{k} \times \mathrm{C}_{k-1}^{p-1}$.
Donc $k\mathrm{C}_k^p = p \times \mathrm{C}_{k-1}^{p-1}$.
Donc $p \mid k\mathrm{C}_k^p$.
Or, comme $1 \leq k \leq p-1$, on a $p \wedge k = 1$.
Donc $d = p \wedge k = 1$. ■

Application 3.3.1.3

1. Si $p \in \mathcal{P}$ tel que $p \mid xy$, alors $p \mid x$ ou $p \mid y$. Car si $p \nmid x$, alors $p \wedge x = 1$, donc $p \mid y$ (théorème de Gauss), et si $p \mid x$, c'est trivial.

3.2 Théorème de Fermat

Théorème 3.3.2.6 *(Théorème de Fermat)*

$$\forall n \in \mathbb{Z}, \forall p \in \mathcal{P}, n^p \equiv n[p]$$

Preuve *(Preuve classique par récurrence)*

■

a faire pour jeudi, çàd dem1

Preuve *(Preuve utilisant des notions de structures algébriques)*

On rappelle que si $(G, \cdot)$ est un groupe fini de cardinal $n \in \mathbb{N}^*$, alors $\forall a \in G, a^n = e$.

On sait que $(\mathbb{U}_{\mathbb{Z}/p\mathbb{Z}}, \times)$ est un groupe fini de cardinal $p-1$.
On a $\forall n \in \mathbb{Z}$, **si** $p \mid n$, alors $\overline{n} = \overline{0}$ et $\overline{n}^p = \overline{0} = \overline{n}$. Cela implique que $n^p \equiv n[p]$.
Le théorème est donc vrai dans ce cas.
Si $p \nmid n$, c'est-à-dire que $n \wedge p = 1$, alors $\overline{n} \in \mathbb{U}_{\mathbb{Z}/p\mathbb{Z}}$.
Donc $\overline{n}^{p-1} = \overline{1}$ (car le cardinal de $\mathbb{U}_{\mathbb{Z}/p\mathbb{Z}}$ est $p-1$).
Cela implique que $\overline{n}^p = \overline{n}$.
D'où $n^p \equiv n[p]$.
Le théorème est donc vrai dans ce cas aussi. ■

Remarque 3.3.2.6

$\forall n \in \mathbb{Z}, \forall k \in \mathbb{N}^* \setminus \{1\}$ tels que $n \wedge k = 1$, alors $n^{\phi(k)} \equiv 1[k]$, où ϕ est la fonction indicatrice d'Euler.
On a aussi : $n \wedge k = 1 \implies \overline{n} \in \mathbb{U}_{\mathbb{Z}/k\mathbb{Z}}$.

Exercice 3.3.2.3

Déterminer le reste de la division euclidienne de 5^{160} par 77.
Solution :
On a $5^{10} \equiv 1[11]$ (car $5 \wedge 11 = 1$ et $\phi(11) = 10$).
Et on a $5^6 \equiv 1[7]$ (car $5 \wedge 7 = 1$ et $\phi(7) = 6$).
Donc on a $5^{160} \equiv 2[7]$ et $5^{160} \equiv 1[11]$.
On peut utiliser le **théorème chinois des restes** pour résoudre ce système. Mais comme celui-ci n'a pas encore été vu, on va procéder par congruences successives.
Nous cherchons $k_0 \in \mathbb{Z}$ tel que $k_0 \equiv \underbrace{1}_{\star}[11]$ et $k_0 \equiv \underbrace{2}_{*}[7]$.
On a $11 \wedge 7 = 1$, donc on peut écrire $11u + 7v = 1$.
Et on a $11 \times 2 + 7 \times (-3) = 1$.
On pose $k_0 = 11 \times 2 \times \underbrace{2}_{*} + 7 \times (-3) \times \underbrace{1}_{\star} = 23$.

Donc $\begin{cases} 5^{160} \equiv 23[11] \\ 5^{160} \equiv 23[7] \end{cases}$
Cela implique que $5^{160} \equiv 23[77]$, sachant que $7 \wedge 11 = 1$.

Théorème 3.3.2.7

Soit $x \in \mathbb{N}^* \setminus \{1\}$. Il existe $p_1, \ldots, p_r \in \mathcal{P}$ tels que $x = \prod_{k=1}^{r} p_k$.

Preuve

Preuve par récurrence (forte) sur $x \in \mathbb{N}^* \setminus \{1\}$.

Initialisation : Pour $x = 2$, on a $2 \in \mathcal{P}$, donc la propriété est vraie.
Hérédité : Supposons que la propriété soit vraie pour tout $k \in \mathbb{N}^* \setminus \{1\}$ tel que $2 \leq k < x$, avec $x \geq 3$.
Si $x + 1 \in \mathcal{P}$, la propriété est vraie.
Sinon, $\exists q \in \mathcal{P}$ tel que $q \mid x + 1$, ce qui implique que $x + 1 = q \times a$ pour un certain $a \in \mathbb{N}^* \setminus \{1\}$ tel que $a < x + 1$.
Cela implique que $a \leq x$, donc en utilisant l'hypothèse de récurrence, on a $a = \prod_{k=1}^{r} p_k$ avec $p_1, \ldots, p_r \in \mathcal{P}$.
Donc $x + 1 = q \times \prod_{k=1}^{r} p_k$, en posant $p_{r+1} = q$. ■

Définition 3.3.2.4 *(Valuation p-adique d'un entier (déf. et théo.))*

Soient $x \in \mathbb{N}^* \setminus \{1\}$ et $p \in \mathcal{P}$.
Il existe un unique $\alpha \in \mathbb{N}$ et un unique $y \in \mathbb{N}^*$ tels que :

$$\begin{cases} x = p^\alpha y \\ p \wedge y = 1 \end{cases}$$

α est appelé la **valuation p-adique** de x, et notée $v_p(x) = \alpha$.

$$v_p(x) = \max\{k \in \mathbb{N} \text{ tel que } p^k \mid x\}$$

Preuve *(Existence et unicité)*

Démonstration de l'existence :
On pose $A = \{k \in \mathbb{N} \text{ tel que } p^k \mid x\}$.
Démonstration de l'unicité :
Supposons que $x = p^{\alpha_1} y_1 = p^{\alpha_2} y_2$ avec $p \wedge y_1 = 1$ et $p \wedge y_2 = 1$.
Supposons que $\alpha_1 \neq \alpha_2$.
On posera $lambda = \alpha_1 - \alpha_2 > 0$ (sans perte de généralité).
On aura donc $p^\lambda y_1 = y_2$.
Ce qui implique que $p \mid y_2$, ce qui est une contradiction, car cela implique que $p = 1$.
On en déduit que $\alpha_1 = \alpha_2$ et $y_1 = y_2$.
■

continue

Propriété 3.3.2.11

Si $x = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i des nombres premiers deux à deux distincts, alors $v_{p_i}(x) = \alpha_i$ pour tout $i \in \{1, \ldots, r\}$, et $v_p(x) = 0$ pour tout $p \in \mathcal{P} \setminus \{p_1, \ldots, p_r\}$.
Et on a $\forall p \in \mathcal{P} \setminus \{p_1, \ldots, p_r\}, v_p(x) = 0$ (les nombres premiers qui ne divisent pas x ont une valuation nulle).

Preuve

On a $\forall i \in \{1,\dots,r\}, x = p_i^{\alpha_i} \cdot \underbrace{\prod_{\substack{k=1 \\ k\neq i}}^{r} p_k^{\alpha_k}}_{=y_i}$.
Les p_k (premiers) sont deux à deux distincts, donc $p_i \wedge \prod_{k=1\ ;\ k\neq i}^{r} p_k^{\alpha_k} = 1$.
Cela implique que $p_i \wedge y_i = 1$ pour tout $i \in \{1,\dots,r\}$.
On en déduit que $v_{p_i}(x) = \alpha_i$ pour tout $i \in \{1,\dots,r\}$.
Soit $p \in \mathcal{P} \setminus \{p_1,\dots,p_r\}$.
On a $x = p^0 \cdot x$, et $p \notin \{p_1,\dots,p_r\} \implies \forall i, p \wedge p_i = 1 \implies p \wedge x = 1$.
Donc $v_p(x) = 0$ pour tout $p \in \mathcal{P} \setminus \{p_1,\dots,p_r\}$. ■

3.3 Décomposition primaire et applications

Théorème 3.3.3.8 *(Décomposition primaire)*

Soit $x \in \mathbb{N}^* \setminus \{1\}$.
Il existe $p_1 < \cdots < p_r \in \mathcal{P}$ deux à deux distincts, et $\alpha_1,\dots,\alpha_r \in \mathbb{N}^*$ tels que $x = \prod_{k=1}^{r} p_k^{\alpha_k}$.
Cette décomposition est unique.
Si on n'impose pas l'ordre $p_1 < \cdots < p_r$, alors la décomposition est unique à l'ordre/la permutation près.
i.e. si $x = \prod_{i=1}^{s} q_i^{\beta_i}$ avec $q_1 < \cdots < q_s \in \mathcal{P}$ et $\beta_j \in \mathbb{N}^* \forall j$, alors $r = s, \forall 1 \leq i \leq r$:
$\begin{cases} p_i = q_i \\ \alpha_i = \beta_i \end{cases}$

Preuve

L'existence a déjà été démontrée.
Démonstration de l'unicité :
Supposons que $x = \prod_{k=1}^{r} p_k^{\alpha_k} = \prod_{i=1}^{s} q_i^{\beta_i}$ avec $\begin{cases} p_1 < \cdots < p_r \in \mathcal{P} \\ q_1 < \cdots < q_s \in \mathcal{P} \end{cases}$ et $\alpha_k, \beta_i \in \mathbb{N}^*$.
Soit $k = 1,\dots,r$. On a $p_k \mid \prod_{i=1}^{s} q_i^{\beta_i}$.
On sait que p_k est premier, donc $\exists i \in \{1,\dots,s\}$ tel que $p_k \mid q_i^{\beta_i} \implies p_k \mid q_i$.
Et on sait aussi que q_i est premier, donc $p_k = q_i$, cela implique que $p_k = 1$ ou $p_k = q_i$.
Donc $\{p_1,\dots,p_r\} \subset \{q_1,\dots,q_s\}$.
De même, on trouve que $\{q_1,\dots,q_s\} \subset \{p_1,\dots,p_r\}$.
Donc $\{p_1,\dots,p_r\} = \{q_1,\dots,q_s\}$, ce qui implique que $r = s$ et $p_i = q_i$ pour tout $i \in \{1,\dots,r\}$.
On a $x = \prod_{k=1}^{r} p_k^{\alpha_k} = \prod_{i=1}^{r} p_i^{\beta_i}$.
D'après la propriété précédente, on a $v_{p_i}(x) = \alpha_i$ et $v_{p_i}(x) = \beta_i$ pour tout $i \in \{1,\dots,r\}$.

Donc $\alpha_i = \beta_i$ pour tout $i \in \{1, \dots, r\}$.
On en déduit que la décomposition primaire de x est unique. ■

Propriété 3.3.3.12

Soient $x, y \in \mathbb{N}^* \setminus \{1\}$.

$$x \mid y \iff \forall p \in \mathcal{P}, v_p(x) \leq v_p(y)$$

Preuve

$(\implies)$: Soit $p \in \mathcal{P}$. On a donc $x = p^\alpha \cdot z_1$ et $p \wedge z_1 = 1$, avec $\alpha = v_p(x)$.
Comme $x \mid y$, on a $y = x \cdot k$ pour un certain $k \in \mathbb{N}$.
De même, il existe un unique $\beta \in \mathbb{N}$, et un unique $z_2 \in \mathbb{N}^*$ tels que $k = p^\beta z_2$ ($\beta = v_p(k)$). On a $p \wedge z_2 = 1$.
Donc $y = p^{\alpha+\beta} z_1 z_2$.
Comme $p \wedge z_1 = 1$ et $p \wedge z_2 = 1$, on a $p \wedge z_1 z_2 = 1$.
Donc $v_p(y) = \alpha + \beta \geq \alpha = v_p(x)$.
$(\impliedby)$: On a $x = \prod_{i=1}^r p_i^{\alpha_i}$ et $y = \prod_{i=1}^r p_i^{\beta_i}$, avec $p_1, \dots, p_r \in \mathcal{P}$ et $\forall 1 \leq i \leq r, \alpha_i, \beta_i \geq 0$.
On a $\forall 1 \leq i \leq r, \alpha_i \leq \beta_i$ (parce que $v_{p_i}(x) \leq v_{p_i}(y)$).
Donc $y = \prod_{i=1}^r p_i^{\beta_i} = \prod_{i=1}^r p_i^{\alpha_i} \cdot \prod_{i=1}^r p_i^{\beta_i - \alpha_i} = x \cdot \underbrace{\prod_{i=1}^r p_i^{\beta_i - \alpha_i}}_{\in \mathbb{N}^*}$.
Donc $x \mid y$. ■

Théorème 3.3.3.9 *(Calcul du PGCD par décomposition primaire)*

Soient $x, y \in \mathbb{N}^* \setminus \{1\}$.
On a $x = \prod_{i=1}^r p_i^{\alpha_i}$ et $y = \prod_{i=1}^r p_i^{\beta_i}$, avec $p_1, \dots, p_r \in \mathcal{P}$ et $\alpha_i, \beta_i \in \mathbb{N}$.
Alors $x \wedge y = \prod_{i=1}^r p_i^{\min(\alpha_i, \beta_i)}$.

Preuve

On pose $d = \prod_{i=1}^r p_i^{m_i}$.
On a $\forall 1 \leq i \leq r, m_i \leq \alpha_i$ et $m_i \leq \beta_i$.
Alors $d \mid x$ et $d \mid y$ donc $d \mid x \wedge y$.
On pose $d' = x \wedge y$, alors $d' \mid x$ et $d' \mid y$.
Donc $\forall p \in \mathcal{P}, \begin{cases} v_p(d') \leq v_p(x) \\ v_p(d') \leq v_p(y) \end{cases}$
i.e. $\forall 1 \leq i \leq r, v_{p_i}(d') \leq \alpha_i$ et $v_{p_i}(d') \leq \beta_i$.
Donc $\forall 1 \leq i \leq r, v_{p_i}(d') \leq \min(\alpha_i, \beta_i) = m_i$.
D'après la propriété précédente, on a $d' \mid d$.
On a $d \mid d'$ et $d' \mid d$, donc $d = d'$, car ils sont tous les deux positifs.

On en déduit que $x \wedge y = \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)}$. ■

Exercice 3.3.3.4

Soient $x, y \in \mathbb{N}^*$. Montrer que $x \mid y \iff x^2 \mid y^2$.
Solution :
On va procéder par équivalences successives en utilisant la propriété 3.3.

$$\begin{aligned} x^2 \mid y^2 &\iff \forall p \in \mathcal{P}, v_p(x^2) \leq v_p(y^2) \\ &\iff \forall p \in \mathcal{P}, 2v_p(x) \leq 2v_p(y) \\ &\iff \forall p \in \mathcal{P}, v_p(x) \leq v_p(y) \\ &\iff x \mid y \text{ CQFD.} \end{aligned}$$

On a utilisé le fait que $v_p(x^2) = 2v_p(x)$ et $v_p(y^2) = 2v_p(y)$, ce qui est une conséquence de la définition de la valuation p-adique (et de la décomposition primaire).

Remarque 3.3.3.7 *(PGCD de a^n, b^n)*

Soient $a, b \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$. Alors

$$a^n \wedge b^n = (a \wedge b)^n.$$

4 Plus petit commun multiple

Définition 4.4.0.5 *(PPCM (déf. et théorème))*

Soient A un anneau principal et $x_1, \dots, x_n \in A$, alors $\exists m \in A$ tel que $\cap_{i=1}^n x_i A = mA$, avec :

$$\forall 1 \leq i \leq n, x_i \mid m \text{ si } M \text{ est un autre multiple commun des } (x_i)_i, \text{ alors } m \mid M$$

m est appelé le **plus petit commun multiple** (PPCM) des x_i et noté $\text{ppcm}(x_1, \dots, x_n)$, ou encore $x_1 \vee x_2 \vee \cdots \vee x_n$.

Preuve

$\forall 1 \leq i \leq n, x_i A$ est un idéal de A.
Donc $\cap_{i=1}^n x_i A$ est un idéal de A, qui est un anneau principal.
$\implies \cap_{i=1}^n x_i A$ est un idéal principal.
i.e. $\exists m \in A$ tel que $\cap_{i=1}^n x_i A = mA$.
Donc $\forall 1 \leq i \leq n, mA \subset x_i A \implies x_i \mid m$.
Si $\exists M$ tel que $\forall 1 \leq i \leq n, x_i \mid M$, alors $M \in x_i A$ pour tout i.
Donc $MA \subset \cap_{i=1}^n x_i A = mA$.
Donc $m \mid M$. ■

Remarque 4.4.0.8

- Si m est un ppcm des x_i, alors les autres ppcm sont les éléments associés à m.
- Dans le cas de $\mathbb{Z}$, le ppcm est unique (on choisit le ppcm positif, ce qu'on appelle le "générateur positif").

Propriété 4.4.0.13

1. $\forall x, y \in \mathbb{Z}, \forall \lambda \in \mathbb{Z}, (\lambda x) \vee (\lambda y) = |\lambda| (x \vee y)$.
2. Si $x, y \in \mathbb{Z}$ tels que $x \wedge y = 1$, alors $x \vee y = |x| \cdot |y|$.
3. $\forall x, y \in \mathbb{Z}, (x \wedge y) \cdot (x \vee y) = |x| \cdot |y|$.

Preuve

Preuve du premier point :

$$\begin{aligned}(\lambda x)\mathbb{Z} \cap (\lambda y)\mathbb{Z} &= (\lambda x \vee \lambda y)\mathbb{Z} \\ \lambda(x\mathbb{Z} \cap y\mathbb{Z}) &= \lambda(x \vee y)\mathbb{Z} \\ (\lambda x \vee \lambda y)\mathbb{Z} &= \lambda(x \vee y)\mathbb{Z} \\ \implies (\lambda x) \vee (\lambda y) &= |\lambda|\,(x \vee y)\end{aligned}$$

Preuve du deuxième point :
On pose $m = x \vee y$.
Donc $x \mid m$ et $y \mid m$.
Comme $x \wedge y = 1$, on a $xy \mid m$ (propriété de l'application).
Et on a $m \mid xy$ (car $m \mid x$ et $m \mid y$).
Donc $m = |xy|$.
Preuve du troisième point :
On pose $d = x \wedge y$, donc $\exists x_1, y_1 \in \mathbb{Z}$ tels que $x = dx_1, y = dy_1$ et $x_1 \wedge y_1 = 1$.
Donc, d'après le deuxième point, on a $x_1 \vee y_1 = |x_1| \cdot |y_1|$.
Donc $d^2(x_1 \vee y_1) = d^2\,|x_1| \cdot |y_1|$.
Donc $|d|\,(dx_1 \vee dy_1) = |dx_1| \cdot |dy_1|$.
Donc $(x \wedge y)(x \vee y) = |x| \cdot |y|$. ■

Théorème 4.4.0.10

Soient $x = \prod_{i=1}^{r} p_i^{\alpha_i}$ et $y = \prod_{i=1}^{r} p_i^{\beta_i}$, avec $p_1, \ldots, p_r \in \mathcal{P}$ et $\alpha_i, \beta_i \in \mathbb{N}$.
Alors $x \vee y = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$.

Preuve

On a $xy = \prod_{i=1}^{r} p_i^{\alpha_i + \beta_i}$.
Or $x \vee y = \frac{xy}{x \wedge y}$.
Donc $x \vee y = \prod_{i=1}^{r} p_i^{\alpha_i + \beta_i - \min(\alpha_i, \beta_i)} = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$.
Sachant que $\alpha_i + \beta_i - \min(\alpha_i, \beta_i) = \max(\alpha_i, \beta_i)$. ■

Fin du Chapitre XI.