# Chapitre 12

# Arithmétique

**12 Arithmétique** **1**
12.1 Propriété fondamentale de $\mathbb{Z}$ . . . . . 2
12.4 Division euclidienne . . . . . 2
12.9 Divisibilité et multiple . . . . . 3
12.10Divisibilité et normes . . . . . 3
12.11Entiers associés . . . . . 3
12.14Intégrité de la divisibilité . . . . . 4
12.20Cas d'une divisibilité . . . . . 4
12.21Préparation à l'algorithme d'Euclide . . . . . 4
12.23Algorithme d'Euclide étendu ou théorème de Bézout . . . . . 4
12.24Application basique . . . . . 5
12.26Théorème de Bézout . . . . . 5
12.28Proposition . . . . . 6
12.29Proposition . . . . . 6
12.30Théorème de Gauss . . . . . 7
12.31Equation de Bézout . . . . . 7
12.32Proposition . . . . . 7
12.37Lien avec les idéaux . . . . . 8
12.38Préparation au calcul pratique d'un *pgcd* . . . . . 8
12.39Caractérisation du *pgcd* . . . . . 8
12.40Propriétés du *pgcd* . . . . . 9
12.44Définition du PPCM . . . . . 10
12.45Caractérisation du *ppcm* . . . . . 10
12.46Propriétés du *ppcm* . . . . . 11
12.50Propriétés . . . . . 12
12.51Petit théorème de Fermat . . . . . 12
12.52Décomposition en produit de facteurs premiers . . . . . 13
12.54Caractérisation de la valuation . . . . . 14
12.55Valuation et décomposition en produit de facteurs premiers . . . . . 14
12.56Propriétés de la valuation . . . . . 14

## 12.1 Propriété fondamentale de $\mathbb{Z}$

**Théorème 12.1**

Toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.

Soit $A$ une partie non vide et minorée de $\mathbb{Z}$.
On note $\mathcal{M}$ l'ensemble des minorants de $A$.
Par hypothèse, $\mathcal{M} \neq \emptyset$.
Supposons par l'absurde que :

$$\forall a \in \mathbb{Z}, a \in \mathcal{M} \Rightarrow a+1 \in \mathcal{M}$$

D'après le principe de récurrence, si $a_0 \in \mathcal{M}$ est fixé :

$$\forall n \geq a_0, n \in \mathcal{M}$$

En particulier, pour $n \in A$ ($A \neq \emptyset$) on a :

$$n \geq a_0 \text{ } (a_0 \text{ est un minorant})$$

Donc $n \in \mathcal{M}$.
Donc $n+1 \in \mathcal{M}$.
Donc $n+1$ est un minorant de $A$.
Donc $n+1 \leq n$.
Absurde.
Ainsi, on choisit $a \in \mathbb{Z}$ avec $a \in \mathcal{M}$ et $a+1 \notin \mathcal{M}$.
On choisit donc $n \in A$ tel que :

$$a \leq n < a+1$$

Donc $n = a \in A$.
Donc $a = \min(A)$.

## 12.4 Division euclidienne

**Théorème 12.4**

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

$$a = bq + r$$

avec $0 \leq r < |b|$. Cette égalité est appelée **division euclidienne de** $a$ **par** $b$, l'entier $q$ est alors appelé **quotient** et l'entier $r$ le **reste**, tandis que $a$ porte le nom de dividende et $b$ celui de diviseur.

Existence :
On suppose dans un premier temps que $b > 0$.
Soit $a \in \mathbb{Z}$.
On note $A = \{n \in \mathbb{Z}, bn \leq a\}$.
$A$ est un sous-ensemble non vide de $\mathbb{Z}$ et majoré.
Il admet donc un plus grand élément, noté $q$. On a donc $q \in A$ et $q+1 \notin A$.

$$bq \leq a < b(q+1)$$
$$\text{donc } 0 \leq a - bq < b$$

On pose alors $r = a - bq$. L'exsitence est alors prouvée pour $b > 0$.
Si $b < 0$, alors $-b > 0$ et on choisit $(q, r) \in \mathbb{Z}^2$ tel que :

$$a = -b \times q + r \text{ avec } 0 \leq r < -b$$

Le couple $(-q, r)$ convient.

Unicité :
On suppose $a = bq + r = bq' + r'$ avec $0 \leq r,' < |b|$.

Donc $b(q-q') = r' - r$.
Donc $\underbrace{|b|}_{>0} \times |q-q'| = |r'-r| < \underbrace{|b|}_{>0}$.
Donc $|q-q'| < 1$.
Donc $q = q'$.
Puis $r = r'$.

## 12.9 Divisibilité et multiple

**Propostion 12.9**

Soit $a$ et $b$ deux entiers. Alors $a$ est divisble par $b$ si et seulement si $a$ est un multiple de $b$.

$\boxed{\Rightarrow}$
Si $b|a$, alors :

$$\begin{aligned} a &= bq + 0 \\ &= bq \\ &\in b\mathbb{Z} \end{aligned}$$

$\boxed{\Leftarrow}$
Si $a \in b\mathbb{Z}$, $a = b \times n = b \times n + 0$.
Par unicité de la division euclidienne, $b|a$.

## 12.10 Divisibilité et normes

**Propostion 12.10**

Soit $a$ et $b$ deux entiers avec $a \neq 0$ et $b|a$. Alors $|b| \leq |a|$.

Si $b|a$, alors $a = b \times n$ avec $n \neq 0$ var $a \neq 0$. Donc :

$$\begin{aligned} |a| &= |b| \times |n| \\ &\geq |b| \times 1 \end{aligned}$$

## 12.11 Entiers associés

**Propostion 12.11**

Soit $a$ et $b$ deux entiers. Alors

$$a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow a = \pm b$$

On dit alors que $a$ et $b$ sont associés.

$\boxed{\Leftarrow}$
Si $a = \pm b$, alors $a\mathbb{Z} = b\mathbb{Z}$.

$\boxed{\Rightarrow}$
Si $a = 0$ et $a\mathbb{Z} = b\mathbb{Z}$, alors $b = 0$.
Si $a \neq 0$ et $a\mathbb{Z} = b\mathbb{Z}$, alors $b \neq 0$ et d'après (12.0) :

$$|a| \leq |b| \text{ et } |b| \leq |a|$$

Donc $|a| = |b|$

## 12.14 Intégrité de la divisibilité

**Propostion 12.14**

Soit $a$, $b$ et $c$ trois entiers, avec $c \neq 0$. Si $nb|na$, alors $n|a$.

Si $cb|ca$, alors $ca = ncb$.
Or $c$ est régulier dans $\mathbb{Z}$ donc :

$$a = nb$$

Donc $b|a$.

## 12.20 Cas d'une divisibilité

**Lemme 12.20**

Si $a|b$, alors

$$\mathcal{D}_{a,b} = \mathcal{D}_a$$

Si $a|b$, si $c|a$, alors $c|b$.
Donc $\mathcal{D}_b \supset \mathcal{D}_a$.
Ainsi, $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_a$

## 12.21 Préparation à l'algorithme d'Euclide

**Lemme 12.21**

Soit $a$, $b$ et $q$ trois entiers, alors

$$\mathcal{D}_{a,b} = \mathcal{D}_{a-bq,b}$$

$\boxed{\subset}$
Soit $n \in \mathcal{D}_{a,b}$, alors :

$$\begin{aligned} n|a \text{ et } n|b \\ \text{donc } n|a - bq \\ \text{donc } n \in \mathcal{D}_{a-bq,b} \end{aligned}$$

$\boxed{\supset}$
Soit $n \in \mathcal{D}_{a-bq,b}$

$$\begin{aligned} n|a - bq \text{ et } n|b \\ \text{donc } n|a - bq + bq \\ \text{soit n|a} \\ \text{donc } n \in \mathcal{D}_{a,b} \end{aligned}$$

## 12.23 Algorithme d'Euclide étendu ou théorème de Bézout

**Lemme 12.23**

Soit $a$ et $b$ deux entiers. Soit $r$ le dernier reste non nul dans l'algorithme d'Euclide appliqué à $a$ et $b$. Il existe deux entiers $u$ et $v$ tels que

$$au + bv = r$$

On utilise les notations du lemme (12.22).
On démontre par récurrence double que :

$$\forall n, \text{"}\exists (u_n, v_n) \in \mathbb{Z}^2, au_n + bv_n = r_n\text{"}$$

Initialisation :
Pour $n = 0$ il s'agit de la division euxlidienne de $a$ par $b$ ($u_0 =$ et $v_0 = -q$).
Pour $n = 1$ :

$$\begin{aligned}
a &= bq + r \\
b &= r \times q_1 + r_1 \\
\text{donc } r &= b - rq_1 \\
&= b - q_1(a - bq) \\
&= -q_1 a + b(1 + q_1 q)
\end{aligned}$$

Hérédité :
On suppose le résultat vrai aux rangs $n$ et $n + 1$.

$$\begin{aligned}
a_n &= b_n q_n + r_n \\
b_n &= r_n q_{n+1} + r_{n+1} \\
r_n &= r_{n+1} q_{n+2} + r_{n+2}
\end{aligned}$$

Donc :

$$\begin{aligned}
r_{n+2} &= r_n - r_{n+1} q_{n+2} \\
&= a u_n + b v_n - (a u_{n+1} + b v_{n+1}) q_{n+2} \\
&= a \underbrace{(u_n - u_{n+1} q_{n+2})}_{\in \mathbb{Z}} + b \underbrace{(v_n - v_{n+1} q_{n+2})}_{\in \mathbb{Z}}
\end{aligned}$$

On utilise le principe de récurrence avec la dernière étape de l'algorithme.

## 12.24 Application basique

**Exemple 12.24**

Appliquer l'algorithme d'Euclide aux entiers 121 et 26.

$$\begin{aligned}
121 &= 26 \times 4 + 17 \\
26 &= 17 \times 1 + 9 \\
17 &= 9 \times 1 + 8 \\
9 &= 8 \times 1 + 1 \\
8 &= 1 \times 8 + 0
\end{aligned}$$

On remonte l'algorithme :

$$\begin{aligned}
1 &= 9 - 8 \\
&= 9 - (17 - 9) \\
&= 2 \times 9 - 17 \\
&= 2 \times (26 - 17) - 17 \\
&= 2 \times 26 - 3 \times 17 \\
&= 2 \times 26 - 3 \times (121 - 4 \times 26) \\
&= 14 \times 26 - 3 \times 121
\end{aligned}$$

## 12.26 Théorème de Bézout

**Théorème 12.26**

Soit $a$ et $b$ deux entiers. Alors $a$ et $b$ sont premiers entre eux si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$au + bv = 1$$

$\boxed{\Rightarrow}$
On suppose $a$ et $b$ premiers entre eux.
Donc $\mathcal{D}_{a,b} = \{\pm 1\}$.
Soit $r$ le dernier reste non nul dans l'algorithme d'Euclide,

$$\mathcal{D}_r = \mathcal{D}_{a,b} = \{\pm 1\}$$

Donc $r = \pm 1$.
D'après le théorème de Bézout, il existe deux entiers $u$ et $v$ tels que :

$$au + bv = 1$$

$\boxed{\Leftarrow}$
Réciproquement, si $au + bv = 1$, alors pour tout $d \in \mathcal{D}_{a,b}$ $d|au + bv$ donc $d|1$ donc $d = \pm 1$.
Donc $\mathcal{D}_{a,b} = \{\pm 1\}$.

## 12.28 Proposition

Propostion 12.28

Si $a$ est premier avec $b$ et $c$, alors $a$ est premier avec $bc$.

D'après le théorème de Bézout, on écrit :

$$\begin{aligned} au_1 + bv_1 &= 1 \\ au_2 + cv_2 &= 1 \end{aligned}$$

avec $(u_1, u_2, v_1, v_2) \in \mathbb{Z}^4$.
Donc :

$$\begin{aligned} 1 &= (au_1 + bv_1)(au_2 + cv_2) \\ &= a\underbrace{(au_1u_2 + bv_1u_2 + cu_1v_2)}_{\in\mathbb{Z}} + \underbrace{v_1v_2}_{\in\mathbb{Z}}bc \end{aligned}$$

Donc $a$ et $bc$ sont premiers entre eux d'après le théorème de Bézout.

## 12.29 Proposition

Propostion 12.29

Si $a$ est premier avec $b$, que $a|c$ et $b|c$, alors $ab|c$.

D'après le théorème de Bézout :

$$au + bv = 1,\ (u, v) \in \mathbb{Z}^2$$

Donc :

$$auc + bvc = c$$

Or $a|c$ et $b|c$, donc :

$$c = ka \text{ et } c = pb$$

Donc :

$$ab\underbrace{[pu + vk]}_{\in\mathbb{Z}} = c$$

Donc $ab|c$.

## 12.30 Théorème de Gauss

**Théorème 12.30**

Si $a|bc$ et que $a$ est premier avec $b$, alors $a|c$.

D'après le théorème de Bézout :

$$au + bv = 1 \text{ avec } (u, v) \in \mathbb{Z}^2$$

Donc $auc + bvc = c$.
Or $a|bc$ donc $a|auc + bvc$.
Soit $a|c$.

## 12.31 Equation de Bézout

**Exemple 12.31**

Résoudre l'équation d'inconnue $(x, y) \in \mathbb{Z}^2, 3x - 2y = 7$.

On remarque que 3 et 2 sont premiers entre eux.

$$\begin{aligned} 3 - 2 &= 1 \\ \text{donc } 3 \times 7 - 2 \times 7 &= 7 \\ \text{donc } (7, 7) &\in \mathcal{S} \end{aligned}$$

On note $(x_0, y_0)$ cette solution.
Soit $(x, y) \in \mathcal{S}$.
Donc :

$$\begin{aligned} 7 &= 3x - 2y \\ 7 &= 3x_0 - 2y_0 \\ \text{donc } 3(x - x_0) &= 2(y - y_0) \end{aligned}$$

Or $3|3(x - x_0)$ et 3 premier avec 2.
Donc $3|y - y_0$.
Donc $y - y_0 = 3k$, avec $k \in \mathbb{Z}$. (Théorème de Gauss)
De la même manière, $x - x_0 = 2l$, avec $l \in \mathbb{Z}$. (Théorème de Gauss)

Réciproquement, soit $x = x_0 + 2l$ et $y = y_0 + 3k$.

$$\begin{aligned} (x, y) \in \mathcal{S} &\Leftrightarrow 7 = 3x - 2y = 3x_0 - 2y_0 + 6l - 6k \\ &\Leftrightarrow 6l - 6k = 0 \\ &\Leftrightarrow k = l \end{aligned}$$

Donc $\mathcal{S} = \{(x_0 + 2k, y_0 + 3k), k \in \mathbb{Z}\}$

## 12.32 Proposition

**Propostion 12.32**

Si $ar \equiv br \mod n$ et si $r$ et $n$ sont premiers entre eux, alors $a \equiv b \mod n$.

Si $ar \equiv br \mod n$, alors $n|r(a - b)$.
Donc $n|a - b$ ($n$ premier avec $r$ et théorème de Gauss).
Donc $a \equiv b \mod n$.

## 12.37 Lien avec les idéaux

**Propostion 12.37**

Soit $a$ et $b$ deux entiers, alors $d$ est le *pgcd* de $a$ et $b$ si et seulement si $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Soit $(a, b) \in \mathbb{Z}^2$. $a\mathbb{Z}$ et $b\mathbb{Z}$ dont des idéaux de $\mathbb{Z}$.
Donc $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc en particulier un sous-groupe de $\mathbb{Z}$.
On choisit donc $d \geq 0$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
Montrons que $d = pgcd(a, b) = a \wedge b$.
D'une part :

$$\begin{aligned}
d &\in d\mathbb{Z} && \text{donc } d = au + bv \text{ (avec } (u,v) \in \mathbb{Z}^2\\
&\in a\mathbb{Z} + b\mathbb{Z} &&\\
\text{or } a \wedge b | a \text{ et } a \wedge b | b & && \text{donc } a \wedge b | au + bv\\
& && \text{soit } a \wedge b | d
\end{aligned}$$

D'autre part, $a \wedge b$ est le dernier reste non nul de l'algorithme d'Euclide, donc (12.23) :

$$\begin{aligned}
a \wedge b &= au + bv \text{ (avec } (u,v) \in \mathbb{Z}^2)\\
&\in a\mathbb{Z} + b\mathbb{Z}\\
&\in d\mathbb{Z}
\end{aligned}$$

Donc $d | a \wedge b$.
Ainsi, $d$ et $a \wedge b$ sont positifs et associés, donc égaux.

## 12.38 Préparation au calcul pratique d'un *pgcd*

**Lemme 12.38**

Si $a$ et $b$ sont tous les deux non nuls, alors pour tout $q \in \mathbb{Z}, pgcd(a, b) = pgcd(a - bq, b)$.

$$\begin{aligned}
\mathcal{D}_{pgcd(a,b)} &= \mathcal{D}_{a,b}\\
&\underset{(12.21)}{=} \mathcal{D}_{a-bq,b}\\
&= \mathcal{D}_{pgcd(a-bq,b)}
\end{aligned}$$

Les deux *pgcd* sont associés, donc égaux car positifs.

## 12.39 Caractérisation du *pgcd*

**Propostion 12.39**

Soit $a$ et $b$ deux entiers et $d \in \mathbb{N}$. Alors $d = pgcd(a, b)$ si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ avec $u$ et $v$ premiers entre eux, tels que $a = du$ et $b = dv$.

$\boxed{\Rightarrow}$
On suppose que $d = a \wedge b$.
Donc $d|a$ et $d|b$.
On écrit donc $a = du$ et $b = dv$ avec $(u, v) \in \mathbb{Z}^2$.
Notons $n = u \wedge v$. On écrit $u = n \times u'$ et $v = n \times v'$ avec $(u', v') \in \mathbb{Z}^2$.
Donc $a = d \times n \times u'$ et $b = d \times n \times v'$.
Donc $dn \in \mathcal{D}_{a,b} = \mathcal{D}_d$.
Donc $dn|d$.
Donc $n = 1$.

$\boxed{\Leftarrow}$
On suppose que $a = du$ et $b = dv$ avec $u \wedge v = 1$.
D'après le théorème de Bézout :

$$uu' + vv' = 1 \text{ (avec } (u', v') \in \mathbb{Z}^2\text{)}$$

Donc $duu' + dvv' = d$.
Soit $au' + bv' = d$.
Donc $d \in a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.
Donc $a \wedge b | d$.
Par ailleurs, $d \in \mathcal{D}_{a,b} = \mathcal{D}_{a \wedge b}$.
Donc $d | a \wedge b$.
Ainsi, $a \wedge b$ et $d$ sont associés (et positifs) donc égaux.

## 12.40 Propriétés du *pgcd*

**Propostion 12.40**

Soit $a$ et $b$ deux entiers tous deux non nuls.

1. pour tout $n \in \mathbb{Z}$, si $n|a$ et $n|b$, alors $n|pgcd(a, b)$ ;
2. pour tout $k \in \mathbb{N}^*, pgcd(ka, kb) = kpgcd(a, b)$ ;
3. pour tout $n \in \mathbb{N}, pgcd(a^n, b^n) = pgcd(a, b)^n$ ;
4. si $a$ et $c$ sont premiers entre eux, alors $pgcd(a, bc) = pgcd(a, b)$.

1. RAF (définition)
2. Soit $k \in \mathbb{N}^*$. On écrit (12.39) :

$$\begin{aligned} a &= (a \wedge b)u \\ b &= (a \wedge b)v \text{ (avec } u \wedge v = 1\text{)} \end{aligned}$$

   Donc :

$$\begin{aligned} ka &= [k(a \wedge b)]\, u \\ kb &= [k(a \wedge b)]\, v \end{aligned}$$

   Donc (12.39) :

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

3. Avec une partie des notations de 2. :

$$\begin{aligned} a^n &= (a \wedge b)^n u^n \\ b^n &= (a \wedge b)^n v^n \end{aligned}$$

   Avec $(u^n) \wedge (v^n) = 1$.
   Donc (12.39) :

$$pgcd(a^n, b^n) = (a \wedge b)^n$$

4. 

$$\begin{aligned} a &= (a \wedge b)u \\ b &= (a \wedge b)v \text{ (avec } u \wedge v = 1\text{)} \end{aligned}$$

   Donc

$$bc = (a \wedge b) \times vc$$

   Or, puisque $a \wedge c = 1$ et que $u|a$, alors :

$$u \wedge c = 1$$

   Donc (12.28) :

$$u \wedge (vc) = 1$$

   Donc (12.39) :

$$pgcd(a, bc) = a \wedge b$$

## 12.44 Définition du PPCM

**Propostion 12.44**

Soit $a$ et $b$ deux entiers non nuls. On appelle **PPCM** (plus petit commun multiple) l'unique entier $m \in \mathbb{N}$ tel que

$$(a\mathbb{Z}) \cap (b\mathbb{Z}) = m\mathbb{Z}.$$

Cet entier est noté $ppcm(a, b)$ ou encore $a \vee b$.

$a\mathbb{Z}$ et $b\mathbb{Z}$ ont des idéaux de $\mathbb{Z}$.
Donc $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc un sous-groupe de $\mathbb{Z}$.
Donc il existe un unique entier $m \in \mathbb{N}$ tel que :

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$$

Comme $a \neq 0$ et $b \neq 0$, alors $m \neq 0$.

## 12.45 Caractérisation du *ppcm*

**Propostion 12.45**

Soit $a$ et $b$ deux entiers, et $m \in \mathbb{N}$. Alors $m = ppcm(a, b)$ si et seulement si il existe $(u, v) \in \mathbb{Z}^2$, premiers entre eux tels que $m = au = bv$.

$\boxed{\Rightarrow}$
On suppose que $m = a \vee b$.
Donc $m \in a\mathbb{Z} \cap b\mathbb{Z}$.
Donc $m = au = bv$.
On note $d = pgcd(u, v)$.
On écrit donc :

$$u = da'$$
$$v = db'$$

Donc :

$$ada' = bdb'$$

Donc :

$$aa' = bb' = m'$$

Donc :

$$\begin{aligned} m' &\in a\mathbb{Z} \cap b\mathbb{Z} \\ &\in m\mathbb{Z} \end{aligned}$$

Donc :

$$dm' = m | m'$$

Donc :

$$d = 1$$

$\boxed{\Leftarrow}$
On suppose que $m = au = bv$ avec $pgcd(u, v) = 1$.
D'une part :

$$m \in a\mathbb{Z} \cap b\mathbb{Z} = ppcm(a, b)\mathbb{Z}$$

Donc :

$$ppcm(a, b) | m$$

D'autre part, d'après le théorème de Bézout :

$$uu' + vv' = 1 \text{ avec } (u', v') \in \mathbb{Z}^2$$

Donc :

$$uu'\underbrace{ppcm(a,b)}_{ka}+vv'\underbrace{ppcm(a,b)}_{qb}=ppcm(a,b)$$

Donc :

$$m(u'k+vq')=ppcm(a,b)$$

Donc $m|ppcm(a,b)$.

## 12.46 Propriétés du *ppcm*

**Propostion 12.46**

Soit $a$ et $b$ deux entier non nuls, alors :

1. pour tout $n\in\mathbb{Z}$, si $a|n$ et $b|n$, alors $ppcm(a,b)|n$ ;
2. si $a$ et $b$ sont premiers entre eux, alors $ppcm(a,b)=|ab|$ ;
3. pour tout $k\in\mathbb{N}^*$, $ppcm(ka,kb)=kppcm(a,b)$ ;
4. $ppcm(a,b)\times pgcd(a,b)=|ab|$ ;
5. pour tout $n\in\mathbb{N}$, $ppcm(a^n,b^n)=ppcm(a,b)^n$.

1. RAF (12.44)
2. On suppose que $a>0$ et $b>0$.

   $$ab=ba$$

   avec $a\wedge b=1$.
   D'après (12.45) :

   $$ppcm(a,b)=ab$$

3. On écrit (12.45) :

   $$ppcm(a,b)=au=bv \text{ (avec } u\wedge v=1)$$

   Alors :

   $$\begin{aligned} b\wedge ppcm(a,b)&=(ak)u\\ &=(bk)v\end{aligned}$$

   Donc (12.45) :

   $$ppcm(ak,bk)=kppcm(a,b)$$

5. Avec les mêmes notations :

   $$\begin{aligned} ppcm(a,b)^n&=a^nu^n\\ &=b^nv^n \text{ (avec } u^n\wedge v^n=1)\end{aligned}$$

   Donc (12.45) :

   $$ppcm(a^n,b^n)=ppcm(a,b)^n$$

4. D'après (12.39) (avec $a>0$ et $b>0$) :

   $$\begin{aligned} a&=pgcd(a,b)u\\ b&=pgcd(a,b)v \text{ (avec } u\wedge v=1)\\ pgcd(a,b)\times ppcm(a,b)&=pgcd(a,b)ppcm(pgcd(a,b)u,pgcd(a,b)v)\\ &\underset{(3.)}{=}pgcd(a,b)^2ppcm(u,v)\\ &\underset{(2.)}{=}pgcd(a,b)^2uv\\ &=ab\end{aligned}$$

## 12.50 Propriétés

Propostion 12.50

1. Si $p \in \mathbb{P}$, alors pour tout $n \in \mathbb{Z}$, soit $p|n$ soit $pgcd(n, p) = 1$.
2. Si $n \geq 2$, alors $n$ possède au moins un diviseur premier.
3. L'ensemble $\mathbb{P}$ est infini.
4. Si $n > 1$ n'as pas de diviseur dans $[2; \sqrt{n}]$, alors $n$ est premier.
5. Si $p \in \mathbb{P}$, alors pour tout $a$ et $b$ entiers, on a $(a+b)^p \equiv a^p + b^p \pmod{p}$.

1. On suppose que $p \not| n$.
   Soit $d \in \mathcal{D}_p \cap \mathcal{D}_n$.
   $d > 0$ et $d \neq p$.
   Donc $d = 1$.
   Donc $p \wedge n = 1$.
2. On raisonne par récurrence forte → cf. (2.41).
3. On suppose par l'absurde que :
   $$\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$$
   On pose :
   $$m = \prod_{i=1}^{n} (p_i) + 1$$
   Soit $p_i \in \mathbb{P}$ tel que $p_i|m$ (12.50.2).
   Donc $p_i|1$.
   Absurde.
4. On suppose $n \notin \mathbb{P}$.
   Soit $n = ab$ avec $a \geq 2$ et $b \geq 2$.
   Si $a > \sqrt{n}$ et $b > \sqrt{n}$, alors $ab = n > \sqrt{n}^2 = n$.
   Absurde.
5. D'après le binôme de Newton :
   $$\begin{aligned}(a+b)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \\ &= a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}\end{aligned}$$
   Or, pour $k \in [\![1; p-1]\!], p\binom{p-1}{k-1} = k\binom{p}{k}$ (formule du capitaine).
   Or $k \wedge p = 1$ et $p \left| p\binom{p-1}{k-1} \right.$ soit $p \left| \binom{p}{k} \right.$.
   Donc :
   $$p \left| \binom{p}{k} \right.$$
   Donc :
   $$(a+b)^p \equiv a^p + b^p \pmod{p}$$

## 12.51 Petit théorème de Fermat

Théorème 12.51

Pour tout $n \in \mathbb{Z}$ et $p \in \mathbb{P}$, on a $n^p \equiv n \pmod{p}$. En outre, si $pgcd(n, p) = 1$, alors $n^{p-1} \equiv 1 \pmod{p}$.

Soit $p \in \mathbb{P}$. On montre le résultat pour $n \geq 0$ par récurrence.
On a bien $0^p = 0 \equiv 0 \pmod{p}$. Si $n^p \equiv n \pmod{p}$, alors :

$$\begin{aligned}(n+1)^p &\equiv n^p + 1^p \pmod{p} \text{ (12.50.5).} \\ &\equiv n + 1 \pmod{p} \text{ (Hypothèse de récurrnce)}\end{aligned}$$

Soit $n \in \mathbb{N}$.

— Si $p \geq 3$ (donc $p$ est impair), alors :

$$\begin{aligned} n^p &\equiv n \pmod p \\ (-n)^p &\underset{p \text{ impair}}{\equiv} -n^p \pmod p \\ &\equiv -n \pmod p \end{aligned}$$

— Si $p = 2$, $-1 \equiv 1 \pmod 2$.
Donc :

$$\begin{aligned} (-n)^2 &\equiv n^2 \pmod 2 \\ &\equiv n \pmod 2 \\ &\equiv -n \pmod 2 \end{aligned}$$

## 12.52 Décomposition en produit de facteurs premiers

**Théorème 12.52**

Soit $n \in \mathbb{Z}\backslash\{-1,0,1\}$, alors il existe des nombres premiers $p_1, \dots, p_r$ tous distincts, et $(\alpha_1, \dots, \alpha_r) \in (\mathbb{N}^*)^r$ et $\epsilon \in \{\pm 1\}$ tels que

$$n = \epsilon p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$$

Cette décomposition est unique à l'ordre près.

<u>Existence :</u>
On montre l'existence par récurrence forte sur $\mathbb{N}\backslash\{0,1\}$.
- RAF si $n = 2$.
- On suppose le résultat vrai pour tout $k \in [\![2;n]\!]$.
  - Si $n+1 \in \mathbb{P}$ : RAF
  - Si $n+1 \notin \mathbb{P}$, on écrit :
  $$n+1 = k \times q \text{ avec } (k,q) \in [\![2,n]\!]^2$$
  Donc $k$ et $q$ sont des produits de facteurs premiers.
  Donc $n+1 = kq$ est aussi un produit de facteurs premiers.
  Le résultat est donc vrai pour tout $n \in \mathbb{N}$ et par extension pour $-n$ ($\epsilon = -1$).

<u>Unicité :</u>
On suppose que :

$$n = \epsilon p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r} = \epsilon' q_1^{\beta_1} \times \dots \times q_s^{\beta_s}$$

Nécessairement, $\epsilon = \epsilon'$.
Soit $p_i \in \{p_1, \dots, m_r\}$.
On a $p_i | n$ donc $p_i \left| q_1^{\beta_1} \times \dots \times q_s^{\beta_s} \right.$.
Il existe $p_i \in \mathbb{P}$ donc $j \in [\![1;s]\!]$ tel que $p_i | q_j$.
Donc $p_i = \underbrace{q_j}_{\in \mathbb{P}}$.
Ainsi :

$$\{p_1, \dots, p_r\} \subset \{q_1, \dots, q_s\}$$

Par symétrie :

$$\{p_1, \dots, p_r\} = \{q_1, \dots, q_s\}$$

Donc $r = s$ et quitte à renommer $q_j$, on peut supposer que :

$$\forall i \in [\![1;r]\!], p_i = q_i$$

$$p_i^{\alpha_i} | n \text{ donc } p_i^{\alpha_i} \left| \prod_{j=1}^{r} p_j^{\beta_j} \right.$$

$$\text{donc } \alpha_i \leq \beta_i$$

Par symétrie, $\alpha_i = \beta_i$.
L'unicité est prouvée.

## 12.54 Caractérisation de la valuation

**Théorème 12.54**

Soit $n \in \mathbb{Z}^*$ et $p \in \mathbb{P}$ et $d \in \mathbb{N}$. Alors $d = v_p(n)$ si et seulement si $n = p^d u$, avec $u \wedge p = 1$.

On a :

$$\begin{aligned} d = v_p(n) &\Leftrightarrow (p^d | n \text{ et } p^{d+1} \not| n) \\ &\Leftrightarrow \exists u \in \mathbb{Z}, n = p^d u \text{ et } p^{d+1} \not| u \\ &\Leftrightarrow \exists u \in \mathbb{Z}, n = p^d u \text{ et } p \not| u \\ &\underset{(p \in \mathbb{P})}{\Leftrightarrow} \exists u \in \mathbb{Z}, n = p^d u \text{ et } u \wedge p = 1 \end{aligned}$$

## 12.55 Valuation et décomposition en produit de facteurs premiers

**Théorème 12.55**

Si $p|n$, alors $v_p(n)$ est la puissance de $p$ intervenant dans la décomposition en produit de facteurs premiers de $n$.

On écrit la décomposition :

$$n = \epsilon \prod_{i=1}^{r} p_i^{\alpha_i}$$

Soit $k \in [\![1, r]\!]$.

$$n = \epsilon \times p_k^{\alpha_k} \times \underbrace{\prod_{i \neq k} p_i^{\alpha_i}}_{:= u \text{ (avec } u \wedge p_k = 1)}$$

Donc (12.54) :

$$\boxed{v_{p_k}(n) = \alpha_k}$$

## 12.56 Propriétés de la valuation

**Propostion 12.56**

Pout tout $(n, m) \in \mathbb{Z}^2$ et $p \in \mathbb{P}$, on a

1. $p|n$ si et seulement si $v_p(n) > 0$ ;
2. $v_p(mn) = v_p(m) + v_p(n)$ ;
3. $v_p(n + m) \geq \min(v_p(n), v_p(m))$ avec égalité si les valuations sont distinctes ;
4. $n|m \Leftrightarrow (\forall q \in \mathbb{P}, v_q(n) \leq v_q(m))$ ;
5. si de plus $n$ et $m$ sont non nuls alors

$$v_p(n \wedge m) = \min(v_p(n), v_p(m)) \text{ et } v_p(n \vee m) = \max(v_p(n), v_p(m)).$$

1. RAF
2. On écrit $m = p^{v_p(m)} \times u$ et $n = p^{v_p(n)} \times v$ avec $u \wedge p = 1 = v \wedge p$ (12.54).
   Donc $mn = p^{v_p(m)+v_p(n)} \times uv$.
   Or $p \wedge (uv) = 1$.
   Donc (12.54) :

$$\boxed{v_p(mn) = v_p(m) + v_p(n)}$$

3. On suppose que $v_p(m) \leq v_p(n)$.
   Ainsi :

$$\begin{aligned} n+m &= p^{v_p(n)} \times v + p^{v_p(m)} \times u \\ &= p^{v_p(m)} \left[ u + v_p^{v_p(n)-v_p(m)} \right] \end{aligned}$$

   Ainsi, $p^{v_p(m)} | n+m$.
   Par définition :

$$\boxed{v_p(m+n) \geq v_p(m) = \min(v_p(m), v_p(n))}$$

   .
   Si on suppose de plus que $v_p(m) \neq v_p(n)$, alors

$$p \wedge (u + v \times p^{v_p(n)-v_p(m)}) = p \wedge u = 1$$

   Donc (12.54) :

$$\boxed{v_p(n+m) = v_p(m) = \min(v_p(m), v_p(n))}$$

4. On a :

$$\begin{aligned} & n|m \text{ ssi la décomposition en produit de facteurs premiers de } n \text{ se retrouve dans celle de } m. \\ & \underset{(12.55)}{\text{ssi}} \text{ pour tout } p \in \mathbb{P} \text{ tel que } p|n, \text{ alors } v_p(n) \leq v_p(m). \\ & \underset{(\text{si } p \nmid n,\, v_p(n) = 0 \leq v_p(m))}{\text{ssi}} \text{ pour tout } \boxed{p \in \mathbb{P}, v_p(n) \leq v_p(m)}. \end{aligned}$$

5. On a $(n \wedge m)|n$ et $(n \wedge m)|m$.
   Donc (12.56.4) $\boxed{v_p(n \wedge m) \leq \min(v_p(n), v_p(m))}$.
   On suppose par exemple que $v_p(n) \leq v_p(m)$.
   Donc $p^{v_p(n)}|n$ et $p^{v_p(n)}|m$.
   Donc $p^{v_p(n)}|n \wedge m$.
   Par définition $\boxed{v_p(n \wedge m) \geq v_p(n)}$.
   Donc :

$$\boxed{v_p(n \wedge m) = \min(v_p(n), v_p(m))}$$

   On rappelle que $(n \wedge m) \times (n \vee m) = |nm|$.
   Donc $v_p((n \wedge m) \times (n \vee m)) = v_p(nm)$.
   Donc (12.56.2) :

$$\begin{aligned} v_p(n \vee m) &= v_p(n) + v_p(m) - v_p(n \wedge m) \\ &= v_p(n) + v_p(m) - \min(v_p(n), v_p(m)) \\ &= \boxed{\max(v_p(n), v_p(m))} \end{aligned}$$

Les preuves ont été rédigées avec les hypothèses $n \neq 0$ et $m \neq 0$. Si l'un des entiers est nul, on vérifie les assertions avec la convention $v_p(0) = +\infty$.