Arithmétique des entiers relatifs

Commençons par une propriété fondamentale de l'ensemble des entiers naturels.

Théorème 0.1

Toute partie non vide et majorée de $\mathbb{N}$ possède un plus grand élément. Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

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

1 Division dans $\mathbb{Z}$

1.1 Relation de divisibilité

Définition 1.1 Divisibilité, diviseur, multiple

Soit $(a, b) \in \mathbb{Z}^2$. On dit que a **divise** b et on note $a \mid b$ s'il existe $k \in \mathbb{Z}$ tel que $b = ka$. Dans ce cas, on dit que a est un **diviseur** de b ou que b est un **multiple** de a.

Remarque. 1 divise tous les entiers. 0 est divisible par tous les entiers.

Proposition 1.1 Propriétés de la divisibilité

Soit $(a, b, c, d) \in \mathbb{Z}^4$.

Réflexivité $a \mid a$.

Transitivité Si $a \mid b$ et $b \mid c$ alors $a \mid c$.

«Pseudo-antisymétrie» Si $a \mid b$ et $b \mid a$, alors $|a| = |b|$.

«Combinaison linéaire» Si $d \mid a$ et $d \mid b$, alors $d \mid au + bv$ pour tout $(u, v) \in \mathbb{Z}^2$.

Produit Si $a \mid b$ et $c \mid d$, alors $ac \mid bd$.
En particulier, si $a \mid b$ alors $a^n \mid b^n$ pour tout $n \in \mathbb{N}$.

Multiplication/division par un entier Si $d \neq 0$, $a \mid b \iff ad \mid bd$.

Attention ! En arithmétique, on travaille sur des entiers. On évite, autant que faire se peut, de manipuler des fractions quand bien même ces fractions seraient entières. Si, par exemple, a divise b, la fraction $\frac{b}{a}$ est bien un entier mais plutôt que de manipuler la fraction $\frac{b}{a}$, il est préférable de définir l'entier k tel que $b = ka$ et de travailler avec cet entier k. Vous verrez que cela vous évitera nombre d'erreurs.

1.2 Relation de congruence

La relation de congruence est une extension de la relation de divisibilité.

Définition 1.2 Congruence

Soient $(a,b) \in \mathbb{Z}^2$ et $n \in \mathbb{N}$. On dit que a et b sont **congrus modulo** n si $n \mid b-a$ i.e. s'il existe $k \in \mathbb{Z}$ tel que $b = a+kn$. On note alors $a \equiv b[n]$.

Remarque. En particulier $a \equiv 0[n]$ signifie que $n \mid a$.

Exercice 1.1

Que signifie $a \equiv 0[2]$ et $a \equiv 1[2]$?

Proposition 1.2 Propriétés de la congruence

Soient $(a,b,c,d) \in \mathbb{Z}^4$ et $n \in \mathbb{N}$.

(i) On dit que la relation de congruence modulo n est une relation d'équivalence car elle vérifie les conditions suivantes.

Réflexivité $a \equiv a[n]$.

Transitivité Si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$.

Symétrie Si $a \equiv b[n]$, alors $b \equiv a[n]$.

(ii) Si $a \equiv b[n]$ et $c \equiv d[n]$, alors $a+c \equiv b+d[n]$.

(iii) Si $a \equiv b[n]$ et $c \equiv d[n]$, alors $ac \equiv bd[n]$. En particulier, si $a \equiv b[n]$, alors $a^k \equiv b^k[n]$ pour tout $k \in \mathbb{N}$.

(iv) Soit $m \in \mathbb{N}^*$. Alors $a \equiv b[n] \iff am \equiv bm[mn]$.

1.3 Division euclidienne

Proposition 1.3 Division euclidienne

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors il **existe un unique** couple d'entiers $(q,r) \in \mathbb{Z} \times \mathbb{N}$ vérifiant :

$$(i) \quad a = bq + r \qquad\qquad (ii) \quad 0 \leq r \leq b-1$$

a s'appelle le **dividende**, b le **diviseur**, q le **quotient**, et r le **reste**.

Attention ! Ne jamais oublier la deuxième condition sinon il n'y a plus unicité.

Remarque. En termes de congruence, on a donc $a \equiv r[b]$. De plus, $q = \lfloor \frac{a}{b} \rfloor$.

Proposition 1.4

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

Sous-groupes de $(\mathbb{Z},+)$

Les sous-groupes de $(\mathbb{Z},+)$ sont les $a\mathbb{Z}$ avec $a \in \mathbb{Z}$. De plus, on a :

(i) $a\mathbb{Z} \subset b\mathbb{Z} \iff b \mid a$.

(ii) $a\mathbb{Z} = b\mathbb{Z} \iff a = \pm b$.

2 Diviseurs et multiples communs

Définition 2.1

Soit $(a,b) \in \mathbb{Z}^2$. On appelle diviseur commun de a et b tout entier qui divise à la fois a et b. On appelle multiple commun de a et b tout entier qui est à la fois multiple de a et multiple de b.

2.1 PGCD d'un couple d'entiers

Définition 2.2 PGCD

Soit $(a,b) \in \mathbb{Z}^2$. On appelle **plus grand commun diviseur (PGCD)** du couple (a,b) tout entier $d \in \mathbb{Z}$ vérifiant :

(i) d est un diviseur commun de a et b i.e. $d \mid a$ ET $d \mid b$;

(ii) tout diviseur commun de a et b divise d i.e. $\forall \delta \in \mathbb{Z}, (\delta \mid a \text{ ET } \delta \mid b) \Rightarrow \delta \mid d$.

Remarque. Le pgcd est le plus grand au sens de la divisibilité : si $(a,b) \in \mathbb{N}^2$, $a \wedge b$ est la borne inférieure de la partie $\{a,b\}$ pour la relation d'ordre que constitue la divisibilité.

Proposition 2.1 Existence et « unicité » du pgcd

Soit $(a,b) \in \mathbb{Z}^2$. Il existe un unique pgcd **positif** de (a,b). On le note $a \wedge b$.
Deux pgcd de (a,b) sont égaux ou opposés.

Remarque. On montre en fait que $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.

Méthode **Prouver que deux couples d'entiers ont le même pgcd**

Soient (a,b) et (c,d) deux couples d'entiers relatifs. Pour montrer que $a \wedge b = c \wedge d$, on peut montrer :

- $a \wedge b$ divise c et d ;
- $c \wedge d$ divise a et b.

Proposition 2.2 Propriétés du pgcd

Soit $(a,b) \in \mathbb{Z}^2$.

(i) Pour tout $k \in \mathbb{Z}$, $ka \wedge kb = |k|(a \wedge b)$.

(ii) Pour tout diviseur commun $d \neq 0$ de a et b, $\dfrac{a}{d} \wedge \dfrac{b}{d} = \dfrac{a \wedge b}{|d|}$.

Lemme 2.1

Soit $(a,b,k) \in \mathbb{Z}^3$. Alors $a \wedge b = a \wedge (b + ka)$.

Remarque. Notamment, si r est le reste de la division euclidienne de a par b, alors $a \wedge b = b \wedge r$.

L'algorithme suivant permet de déterminer le pgcd de deux entiers par une succession de divisions euclidiennes.

Algorithme d'Euclide

On définit une suite (r_n) de la manière suivante :

1. On pose $r_0 = a$ et $r_1 = b$.
2. Pour $n \geq 1$, r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n.

(r_n) est une suite strictement décroissante d'entiers naturels (à partir du rang 1) : elle est donc nulle à partir d'un certain rang. Soit N l'indice du dernier terme non nul. Le lemme précédent montre que

$$a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_\mathrm{N} \wedge r_{\mathrm{N}+1} = r_\mathrm{N} \wedge 0 = r_\mathrm{N}$$

Exemple 2.1

Déterminons le pgcd de 150 et 54.

$$\begin{aligned}
150 &= 2 \times 54 + 42 \\
54 &= 1 \times 42 + 12 \\
42 &= 3 \times 12 + 6 \\
12 &= 2 \times 6 \quad + 0
\end{aligned}$$

On a donc $150 \wedge 54 = 6$.

Implémentation de l'algorithme d'Euclide

On peut proposer la fonction Python suivante.

```
def euclide(a, b):
        while b != 0:
                a, b = b, a % b
        return abs(a)    # Le PGCD est positif par définition
```

```
>>> euclide(150, 54), euclide(156, -180)
(6, 12)
```

La relation $a \wedge b = b \wedge r$ permet également de donner une version récursive de cet algorithme.

```
def euclide_rec(a, b):
    return abs(a) if b == 0 else euclide_rec(b, a % b)   # Le PGCD est positif par
     ↪   définition
```

```
>>> euclide_rec(150, 54), euclide_rec(156, -180)
(6, 12)
```

Théorème 2.1 Bézout

Soit $(a, b) \in \mathbb{Z}^2$. Il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = a \wedge b$. On appelle (u, v) un couple de **coefficients de Bézout**. Une égalité du type précédent s'appelle une **identité de Bézout**.

Attention ! Ces coefficients ne sont pas uniques. Si (u_0, v_0) est un couple de coefficients de Bézout, tous les couples de la forme $(u_0 + kb, v_0 - ka)$ avec $k \in \mathbb{Z}$ le sont aussi.

Remarque. La réciproque de ce théorème est fausse. Ainsi $6 = 6 \times 6 - 2 \times 15$ mais $6 \wedge 15 \neq 6$. Néanmoins, on a le résultat suivant pour $(a, b, d) \in \mathbb{Z}^3$.

$$\big(\exists (u,v) \in \mathbb{Z}^2,\ au + bv = d\big) \iff a \wedge b \mid d$$

Algorithme d'Euclide étendu

On reprend les notations de l'algorithme d'Euclide. Pour tout $n \geq 1$, on a $r_{n+1} = r_n - q_n r_{n-1}$. Le dernier reste non nul r_{N} est le pgcd d de a et b. On abrégera combinaison linéaire à coefficients entiers en CLE. On peut ainsi exprimer d comme une CLE de $r_{\mathrm{N}-1}$ et $r_{\mathrm{N}-2}$. Puis comme on peut exprimer $r_{\mathrm{N}-1}$ comme une CLE de $r_{\mathrm{N}-2}$ et $r_{\mathrm{N}-3}$, on peut exprimer d comme une CLE de $r_{\mathrm{N}-2}$ et $r_{\mathrm{N}-3}$, etc... Finalement on peut exprimer d comme une CLE de $r_0 = a$ et $r_1 = b$. Plutôt qu'un long discours, reprenons l'exemple traité pour l'algorithme d'Euclide standard.

Exemple 2.2

Réécrivons les divisions euclidiennes de l'algorithme d'Euclide standard sous une autre forme :

$$\begin{aligned}
42 &= 150 - 2 \times 54 \\
12 &= 54 \quad - 1 \times 42 \\
6 &= 42 \quad - 3 \times 12
\end{aligned}$$

On part ensuite du pgcd (c'est-à-dire 6) et on remonte les lignes de la manière suivante :

$$\begin{aligned}
6 &= 42 - 3 \times 12 \\
&= 42 - 3 \times (54 - 1 \times 42) = 4 \times 42 - 3 \times 54 \\
&= 4 \times (150 - 2 \times 54) - 3 \times 54 = 4 \times 150 - 11 \times 54
\end{aligned}$$

Et voilà notre identité de Bézout.

Remarque. Pour des entiers «petits», il peut être plus rapide de déterminer les coefficients de Bézout par tatônnements plutôt que par l'algorithme précédent.

Implémentation de l'algorithme d'Euclide étendu

On souhaite déterminer des couples d'entiers (u_n, v_n) tels que

$$au_n + bv_n = r_n$$

Puisque $r_0 = a$ et $r_1 = b$, on pose

$$u_0 = 1 \qquad v_0 = 0 \qquad u_1 = 0 \qquad v_1 = 1$$

On sait que r_{n+2} est le reste de la division euclidienne de r_n par r_{n+1}, c'est-à-dire

$$r_n = q_n r_{n+1} + r_{n+2}$$

ou encore

$$au_n + bv_n = q_n(au_{n+1} + bv_{n+1}) + au_{n+2} + bv_{n+2}$$

On peut donc poser

$$u_{n+2} = u_n - q_n u_{n+1} \qquad v_{n+2} = v_n - q_n v_{n+1}$$

On en déduit la fonction Python suivante.

```python
def bezout(a, b):
    u, v, uu, vv = 1, 0, 0, 1
    while b != 0:
        a, b, q = b, a % b, a // b
        u, v, uu, vv = uu, vv, u - q * uu, v - q * vv
    return (-uu, -vv) if a < 0 else (uu, vv)     # Le PGCD est positif par définition
```

```python
>>> bezout(150, 54), bezout(156, -180)
((-9, 25), (-15, -13))
```

On peut également proposer une version récursive. Si $a = bq + r$ est la division euclidienne de a par b et si on connaît $(u, v) \in \mathbb{Z}^2$ tel que $ub + vr = b \wedge r$, alors

$$a \wedge b = b \wedge r = ub + vr = ub + v(a - bq) = va + (u - qv)b$$

```python
def bezout_rec(a,b):
    if b == 0:
      return (-1, 0) if a < 0 else (1, 0)    # Le PGCD est positif par définition
    q, r = a // b, a % b
    u, v = bezout_rec(b, r)
    return v, u-q*v
```

```python
>>> bezout_rec(150, 54), bezout_rec(156, -180)
((4, -11), (7, 6))
```

2.2 Couples de nombres premiers entre eux

Définition 2.3 Nombres premiers entre eux

Soit $(a, b) \in \mathbb{Z}^2$. On dit que a et b sont premiers entre eux si leurs seuls diviseurs communs sont ± 1 i.e. si $a \wedge b = 1$.

Il est souvent plus facile de manipuler deux entiers premiers entre eux que deux entiers quelconques dans les exercices.

Méthode **Se ramener à des nombres premiers entre eux**

Soient $(a, b) \in \mathbb{Z}^2$ et $d = a \wedge b$. Il existe $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$. Alors $a' \wedge b' = 1$ i.e. a' et b' sont premiers entre eux.

Proposition 2.3 Forme irréductible d'un rationnel

Soit $r \in \mathbb{Q}$. Alors il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{p}{q}$ et $p \wedge q = 1$.

Théorème 2.2 Bézout

Soit $(a, b) \in \mathbb{Z}^2$. Alors a et b sont premiers entre eux si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Remarque. Contrairement au premier théorème de Bézout, on a bien ici une **équivalence**.

Exemple 2.3

Deux entiers consécutifs sont premiers entre eux. En effet, pour $n \in \mathbb{Z}$, $1 \times (n+1) + (-1) \times n = 1$. Le théorème de Bézout permet alors d'affirmer que n et $n+1$ sont premiers entre eux.

Exercice 2.1

Montrer que $(2n+1) \wedge (2n+3) = 1$ pour tout $n \in \mathbb{Z}$.

Définition 2.4 Inversibilité modulo un entier

Soit $n \in \mathbb{N}^*$. On dit que $a \in \mathbb{Z}$ est **inversible modulo** n s'il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1[n]$.

Proposition 2.4

Soit $n \in \mathbb{N}^*$. Alors $a \in \mathbb{Z}$ est inversible modulo n si et seulement si $a \wedge n = 1$.

Remarque. Si $a \wedge n = 1$, on peut trouver à l'aide de l'algorithme d'Euclide étendu un couple $(u, v) \in \mathbb{Z}^2$ tel que $au + nv = 1$. On a alors $au \equiv 1[n]$ de sorte que u est un inverse de a modulo n.

Méthode **Utilisation d'un inverse pour résoudre une congruence**

Soit $(a, c, n) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $a \wedge n = 1$. Pour résoudre l'équation $ax \equiv c[n]$ d'inconnue $x \in \mathbb{Z}$, il suffit de mutiplier par un inverse b de a modulo n. En effet

$$ax \equiv c[n] \iff bax \equiv bc[n] \iff x \equiv bc[n]$$

Exemple 2.4

Soit à résoudre $8x \equiv 7[45]$. Comme $8 \wedge 45 = 1$, 8 est inversible modulo 45. A l'aide de l'algorithme d'Euclide étendu, on obtient $17 \times 8 - 3 \times 45 = 1$ donc $17 \times 8 \equiv 1[45]$. Finalement

$$8x \equiv 7[45] \iff x \equiv 17 \times 7[45] \iff x \equiv 119[45] \iff x \equiv 29[45]$$

L'ensemble des solutions est donc $29 + 45\mathbb{Z}$.

Théorème 2.3 Gauss

Soit $(a, b, c) \in \mathbb{Z}^3$. Si $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$.

Proposition 2.5

Soient $(a_1, \dots, a_r) \in \mathbb{Z}^r$ et $n \in \mathbb{Z}$.

1. Si $a_1, \dots, a_r$ sont tous premiers avec n, alors le produit $a_1 \dots a_r$ est également premier avec n.
2. Si $a_1, \dots, a_r$ sont premiers entre eux deux à deux et divisent n, alors le produit $a_1 \dots a_r$ divise également n.

Méthode **Equations diophantiennes $ax + by = c$**

On appelle **équation diophantienne** toute équation à inconnues entières. Pour résoudre l'équation $ax + by = c$, d'inconnues $x, y \in \mathbb{Z}$ et de coefficients $a, b, c \in \mathbb{Z}$, on procède de la manière suivante :

Simplification par le pgcd de a et b On calcule $d = a \wedge b$. Si d ne divise pas c, alors il n'y a pas de solutions. Sinon on divise l'équation par d et on aboutit à l'équation $a'x + b'y = c'$ avec a' et b' premiers entre eux.

Recherche d'une solution particulière Soit il existe une solution particulière évidente, soit on la trouve en écrivant une relation de Bézout entre a' et b'.

Recherche de la solution générale Soit (x_0, y_0) une solution particulière. Ainsi (x, y) est solution si et seulement si $a'(x - x_0) + b'(y - y_0) = 0$. Une utilisation judicieuse du théorème de Gauss permet de conclure que les solutions sont les couples $(x_0 + kb', y_0 - ka')$ avec k décrivant $\mathbb{Z}$.

2.3 PPCM d'un couple d'entiers

Définition 2.5 PPCM

Soit $(a, b) \in \mathbb{Z}^2$. On appelle **plus petit commun multiple** du couple (a, b) tout entier $m \in \mathbb{Z}$ vérifiant :

(i) m est un multiple commun de a et b i.e. $a \mid m$ et $b \mid m$;

(ii) tout multiple commun de a et b est multiple de m i.e. $\forall \mu \in \mathbb{Z}, (a \mid \mu \text{ ET } b \mid \mu) \Rightarrow m \mid \mu)$.

Remarque. Le ppcm est le plus petit au sens de la divisibilité : si $(a, b) \in \mathbb{N}^2$, $a \vee b$ est la borne supérieure de la partie $\{a, b\}$ pour la relation d'ordre que constitue la divisibilité.

Proposition 2.6 Existence et « unicité » du PPCM

Soit $(a, b) \in \mathbb{Z}^2$. Il existe un unique ppcm **positif** de (a, b). On le note $a \vee b$.
Deux ppcm de (a, b) sont égaux ou opposés.

Remarque. On montre en fait que $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

Méthode **Prouver que deux couples d'entiers ont le même ppcm**

Soient (a, b) et (c, d) deux couples d'entiers relatifs. Pour montrer que $a \wedge b = c \wedge d$, on peut montrer :

- a et b divisent $c \vee d$;
- c et d divisent $a \vee b$.

Proposition 2.7 Lien entre PGCD et PPCM

Soit $(a, b) \in \mathbb{Z}^2$. Alors $(a \wedge b)(a \vee b) = |ab|$.

Proposition 2.8 Propriétés du ppcm

Soit $(a, b) \in \mathbb{Z}^2$.

(i) Pour tout $k \in \mathbb{Z}$, $ka \vee kb = |k|(a \vee b)$.

(ii) Pour tout diviseur commun $d \neq 0$ de a et b, $\dfrac{a}{d} \vee \dfrac{b}{d} = \dfrac{a \vee b}{d}$.

3 Nombres premiers

3.1 Définition et propriétés

Définition 3.1 Nombre premier, nombre composé

Soit $p \in \mathbb{N}$. On dit que p est **premier** si $p \neq 1$ et si ses seuls diviseurs positifs sont 1 et p.

Remarque. 2 est le seul nombre premier pair.

Remarque. Deux nombres premiers distincts sont premiers entre eux.

Crible d'Eratosthène

On souhaite déterminer tous les nombres premiers compris entre 0 et un entier $n \geq 2$. On élimine de la liste de ces entiers ceux qui ne sont pas premiers de la manière suivante.

- On constate que 0 et 1 ne sont pas premiers.
- On élimine tous les entiers multiples de 2.
- On élimine ensuite tous les entiers mutiples de 3. On peut commencer à $9 = 3 \times 3$ car $6 = 2 \times 3$ est un mutiple de 2 donc il a déjà été éliminé.
- …
- On élimine tous les multiples de d si d n'a pas déjà été identifié comme un nombre non premier. On peut commencer à d^2 car les multiples de d précédents ont déjà été éliminés.
- On arrête dès que $d > \sqrt(n)$. En effet, un entier possède toujours un diviseur inférieur ou égal à $\sqrt{n}$.

```python
from math import sqrt

def eratosthene(n):
    premiers = [False, False] + [True] * (n-1)
    m = int(sqrt(n))
    for d in range(2, m+1):
        if premiers[d]:
            for i in range(d*d, n+1, d):
                premiers[i] = False
    return premiers
```

```python
>>> list(enumerate(eratosthene(20)))
[(0, False), (1, False), (2, True), (3, True), (4, False), (5, True), (6, False), (7,
↪ True), (8, False), (9, False), (10, False), (11, True), (12, False), (13, True), (14,
↪ False), (15, False), (16, False), (17, True), (18, False), (19, True), (20, False)]
```

Proposition 3.1

Soit p un nombre premier et $a \in \mathbb{Z}$. Alors a et p sont premiers entre eux si et seulement si p ne divise pas a.

Remarque. En particulier si p est premier et si $0 < a < p$, a et p sont premiers entre eux.

Attention ! Il est essentiel que p soit premier.

- 4 et 10 ne sont pas premiers entre eux mais 4 ne divise pas 10.
- 1 et 4 sont premiers entre eux mais 1 divise 4.

Proposition 3.2 Lemme d'Euclide

Soient p un nombre premier et $(a, b) \in \mathbb{Z}^2$. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Remarque. Cette proposition se généralise par récurrence au cas de plusieurs entiers.

Théorème 3.1 Théorème de Fermat

Soit p un nombre premier et $a \in \mathbb{Z}$. Montrer que $a^p \equiv a[p]$.
De plus, si $a \wedge p = 1$, alors $a^{p-1} \equiv 1[p]$.

Proposition 3.3

Tout entier $n > 1$ admet un diviseur premier.

Corollaire 3.1

L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Corollaire 3.2

Deux entiers sont premiers entre eux si et seulement si ils n'admettent aucun diviseur premier commun.

3.2 Décomposition en facteurs premiers

Théorème 3.2 Théorème fondamental de l'arithmétique

Soit $n \in \mathbb{N}^*$. Il existe une unique famille $(v_p(n))_{p\in\mathcal{P}}$ d'entiers naturels presque nulle (i.e. dont tous les éléments sont nuls sauf un nombre fini d'entre eux) telle que $n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$.

Pour $p \in \mathcal{P}$, $v_p(n)$ s'appelle la **valuation p-adique** de n. C'est le plus grand entier k tel que p^k divise n.

Exemple 3.1

$1200 = 2^4 \times 3 \times 5^2$ donc $v_2(1200) = 4$, $v_3(1200) = 1$, $v_5(1200) = 2$ et $v_p(1200) = 0$ pour tout $p \in \mathcal{P} \setminus \{2, 3, 5\}$.

Proposition 3.4 Propriétés de la valuation p-adique

Soit p un nombre premier.

- $\forall (m,n) \in (\mathbb{N}^*)^2,\ v_p(mn) = v_p(m) + v_p(n)$.
- $\forall (n,k) \in \mathbb{N}^* \times \mathbb{N},\ v_p(n^k) = kv_p(n)$.

Proposition 3.5 Caractérisation de la divisibilité, du pgcd et du ppcm par les valuations p-adiques

Soit $(a,b) \in (\mathbb{N}^*)^2$.

(i) $a \mid b \iff \forall p \in \mathcal{P},\ v_p(a) \leq v_p(b)$.

(ii) $\forall p \in \mathcal{P},\ v_p(a \wedge b) = \min(v_p(a), v_p(b))$.

(iii) $\forall p \in \mathcal{P},\ v_p(a \vee b) = \max(v_p(a), v_p(b))$.

Remarque. Il s'ensuit que :

(i) $a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$.

(ii) $a \vee b = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$.

Remarque. On retrouve la méthode qu'on emploie intuitivement pour déterminer le PGCD et le PPCM de deux nombres.

4 Compléments

4.1 PGCD d'un nombre fini d'entiers

Définition 4.1 PGCD

Soit $(a_1, \dots, a_r) \in \mathbb{Z}^r$. On appelle **plus grand commun diviseur (PGCD)** de $(a_1, \dots, a_r)$ tout entier $d \in \mathbb{Z}$ vérifiant :

(i) d est un diviseur commun des a_i ;

(ii) tout diviseur commun des a_i est un diviseur de d.

Proposition 4.1 Existence et « unicité » du pgcd

Soit $(a_1, \dots, a_r) \in \mathbb{Z}^r$. Il existe un unique pgcd **positif** de $(a_1, \dots, a_r)$. On le note $a_1 \wedge \dots \wedge a_r$.
Deux pgcd de $(a_1, \dots, a_r)$ sont égaux ou opposés.

Remarque. On montre en fait que $\sum_{i=1}^{r} a_i\mathbb{Z} = (a_1 \wedge \dots \wedge a_r)\mathbb{Z}$.

Proposition 4.2 « Associativité » du PGCD

Soit $(a, b, c) \in \mathbb{Z}^3$. Alors $a \wedge b \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c)$.

Méthode **Calcul du PGCD**

Pour calculer le PGCD d'un nombre fini d'entiers, on peut se ramener à des PGCD de deux entiers. Par exemple

$$10 \wedge 12 \wedge 18 = (10 \wedge 12) \wedge 18 = 2 \wedge 18 = 2$$

ou encore

$$10 \wedge 12 \wedge 18 = 10 \wedge (12 \wedge 18) = 10 \wedge 6 = 2$$

Proposition 4.3 Propriétés du pgcd

Soit $(a_1, \dots, a_r) \in \mathbb{Z}^r$.

(i) Pour tout $k \in \mathbb{Z}$, $(ka_1) \wedge \dots \wedge (ka_r) = |k|(a_1 \wedge \dots \wedge a_r)$.

(ii) Pour tout diviseur commun $d \neq 0$ des a_i, $\frac{a_1}{d} \wedge \dots \wedge \frac{a_r}{d} = \frac{a_1 \wedge \dots \wedge a_r}{|d|}$.

Théorème 4.1 Bézout

Soit $(a_1, \dots, a_r) \in \mathbb{Z}^r$. Il existe $(u_1, \dots, u_r) \in \mathbb{Z}^r$ tel que $\sum_{i=1}^{r} u_i a_i = a_1 \wedge \dots \wedge a_r$.

4.2 Entiers premiers entre eux dans leur ensemble

Définition 4.2 Entiers premiers entre eux dans leur ensemble

Soit $(a_1, \dots, a_r) \in \mathbb{Z}^r$. On dit que $a_1, \dots, a_r$ sont premiers entre eux dans leur ensemble si $a_1 \wedge \dots \wedge a_r = 1$.

Attention ! Si les a_i sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble mais la réciproque est fausse.
Par exemple, $6, 10, 15$ sont premiers entre eux dans leur ensemble sans être premiers entre eux deux à deux.

Théorème 4.2 Bézout

Soit $(a_1, \dots, a_r) \in \mathbb{Z}^r$. Alors $a_1 \wedge \dots \wedge a_r = 1$ si et seulement si il existe $(u_1, \dots, u_r) \in \mathbb{Z}^r$ tel que $\sum_{i=1}^{r} a_i u_i = 1$.

Proposition 4.4

Soit $(a_1, \dots, a_r) \in \mathbb{Z}^r$. Alors $a_1 \wedge \dots \wedge a_r = 1$ si et seulement si il existe $a_1, \dots, a_r$ n'admettent aucun diviseur premier commun.

4.3 PPCM d'un nombre fini d'entiers (hors programme)

Définition 4.3 PPCM (hors programme)

Soit $(a_1, \dots, a_r) \in \mathbb{Z}^r$. On appelle **plus petit commun multiple (PPCM)** de $(a_1, \dots, a_r)$ tout entier $m \in \mathbb{Z}$ vérifiant :

(i) m est un multiple commun des a_i ;

(ii) tout multiple commun des a_i est un multiple de m.

Proposition 4.5 Existence et « unicité » du ppcm (hors programme)

Soit $(a_1, \dots, a_r) \in \mathbb{Z}^r$. Il existe un unique ppcm **positif** de $(a_1, \dots, a_r)$. On le note $a_1 \vee \dots \vee a_r$.
Deux ppcm de $(a_1, \dots, a_r)$ sont égaux ou opposés.

Remarque. On montre en fait que $\bigcap_{i=1}^{r} a_i\mathbb{Z} = (a_1 \wedge \dots \wedge a_r)\mathbb{Z}$.

Proposition 4.6 « Associativité » du PPCM (hors programme)

Soit $(a, b, c) \in \mathbb{Z}^3$. Alors $a \vee b \vee c = (a \vee b) \wedge c = a \vee (b \vee c)$.

Méthode **Calcul du PPCM**

Pour calculer le PPCM d'un nombre fini d'entiers, on peut se ramener à des PPCM de deux entiers. Par exemple

$$10 \vee 12 \vee 18 = (10 \vee 12) \vee 18 = 60 \vee 18 = 180$$

ou encore

$$10 \vee 12 \vee 18 = 10 \vee (12 \vee 18) = 10 \vee 36 = 180$$

Proposition 4.7 Propriétés du ppcm (hors programme)

Soit $(a_1, \dots, a_r) \in \mathbb{Z}^r$.

(i) Pour tout $k \in \mathbb{Z}$, $(ka_1) \vee \dots \vee (ka_r) = |k|(a_1 \vee \dots \vee a_r)$.

(ii) Pour tout diviseur commun $d \neq 0$ des a_i, $\dfrac{a_1}{d} \vee \dots \vee \dfrac{a_r}{d} = \dfrac{a_1 \vee \dots \vee a_r}{|d|}$.

4.4 Valuations p-adiques (hors programme)

Proposition 4.8 Cas d'un nombre fini d'entiers (hors programme)

Soit $(a_1, \dots, a_r) \in (\mathbb{N}^*)^r$.

(i) $\forall p \in \mathcal{P},\ v_p(a_1 \wedge \dots \wedge a_r) = \min(v_p(a_1), \dots v_p(a_r))$.

(ii) $\forall p \in \mathcal{P},\ v_p(a_1 \vee \dots \vee a_r) = \max(v_p(a_1), \dots v_p(a_r))$.