ARITHMETIQUE DANS $\mathbb{Z}$

1 Multiples et diviseurs d'un entier relatif

1.1 Définitions

Propriété 1 L'ensemble $\mathbb{Z}$ muni de l'addition et de la multiplication est un anneau commutatif intègre.

Définition 1 Soient $a, b \in \mathbb{Z}$, on dit que a est un diviseur de b ou que b est un multiple de a s'il existe $k \in \mathbb{Z}$ tel que $b = ka$.

Notations
On note a est un diviseur de b sous la forme $a|b$ (a divise b).
L'ensemble des diviseurs de a dans $\mathbb{Z}$ est noté $\mathcal{D}(a)$, l'ensemble des multiples de a est noté $a\mathbb{Z}$.

Exemple 1
* 1 et -1 divisent tous les entiers.
* 0 est multiple de tous les entiers, mais n'est diviseur que de lui même.
* $\mathcal{D}(5) = \{\pm 1, \pm 5\}$.
* $\mathcal{D}(8) = \{\pm 1, \pm 2, \pm 4, \pm 8\}$.

Remarque 1 La relation | est une relation d'ordre sur $\mathbb{N}$ mais pas sur $\mathbb{Z}$

Proposition 1
1. $\forall a \in \mathbb{Z},\ a|a$.
2. $\forall (a, b) \in \mathbb{Z}^2,\ (a|b \text{ et } b|a) \Leftrightarrow |a| = |b|)$ et non $a = b$.
3. $\forall (a, b, c) \in \mathbb{Z}^3,\ (a|b \text{ et } b|c) \Rightarrow a|c$. La relation | n'est pas antisymétrique sur $\mathbb{Z}$.

1.2 Division euclidienne

Théorème 2 division euclidienne dans $\mathbb{Z}$
Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ avec $0 \leq r < |b|$

Exemple 2 $a = 17$, $b = 5$. $17 = 5 \times 3 + 2,\ q = 3,\ r = 2$.
$a = -17$, $b = 5$. $-17 = 5 \times (-4) + 3,\ q = -4,\ r = 3$.
Il faut bien prendre garde que $r \geq 0$.

Remarque 2 a) On a $q = E(\frac{a}{b})$ et $r = a - bq$.
b) On a $b|a \Longleftrightarrow r = 0$.

2 Plus grand commun diviseur, plus petit commun multiple

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

Proposition 3 Les sous groupes de $(\mathbb{Z}, +)$ sont les sous ensembles $n\mathbb{Z},\ n \in \mathbb{N}$.

Remarque 3 Ce sont également les idéaux de l'anneau $\mathbb{Z}$.

2.2 PGCD de deux entiers

On a $\mathcal{D}(0) \cap \mathbb{N} = \mathbb{N}$ et si $n \in \mathbb{Z}^*$ l'ensemble $\mathcal{D}(n)$ a un plus grand élément, $|n|$.
Si a et b sont des entiers de $\mathbb{Z}$, l'un d'entre eux au moins étant non nul, l'ensemble $\mathcal{D}(a) \cap \mathcal{D}(b)$ est fini non vide $1 \in \mathcal{D}(a) \cap \mathcal{D}(b)$.
Il a donc un plus grand élément.

Définition 2 Soient a et b deux entiers de $\mathbb{Z}$, l'un d'entre eux au moins étant non nul. L'ensemble $\mathcal{D}(a) \cap \mathcal{D}(b)$ des diviseurs communs de a et b a un plus grand élément, appelé pgcd de ces entiers et noté $a \wedge b$.

Remarque 4 Le module **fractions** Python contient une fonction **gcd** permmettant le calcul du pgcd de deux entiers.

```
from fractions import gcd

gcd(1155,910)
35
```

Propriété 2 1. $a \in \mathbb{N}^*$, $a \wedge 0 = a$, $a \wedge 1 = 1$.

2. $a, b \in \mathbb{Z}$, $a \wedge b = b \wedge a$.
3. $a, b \in \mathbb{Z}$, $a \wedge b$ est un diviseur commun à a et à b.
4. $a, b \in \mathbb{Z}$, $a \wedge b = |a| \Longleftrightarrow a|b$.
5. $a, b \in \mathbb{Z}$, $a \wedge b = |a| \wedge |b|$.

2.3 Algorithme d'Euclide

Proposition 4 a) Soient a, b, q trois entiers relatifs. On a $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(a - bq)$, les diviseurs communs de a et de b sont ceux de b et de $a - bq$.
b) Soit $a, b \in Z$, $a = bq + r$ avec $0 \leq r < |b|$ la division euclidienne de a par b. On a $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$

Propriété 3 Algorithme d'Euclide :recherche du pgcd de deux nombres a et b entiers naturels

$$\begin{array}{rcl} \exists!(q_1, r_1) & \in & \mathbb{N}^2 \quad a = bq_1 + r_1 \quad avec \quad 0 \leq r_1 < b \\ si\ r_1 & \neq & 0 \quad alors \quad a \wedge b = b \wedge r_1 \ ; si \ r_1 = 0 \ \ alors \ \ a \wedge b = b \end{array}$$

$p\gcd(a, b)$ est le dernier reste non nul de la suite des restes des divisions successives des dividendes par les restes .On peut augmenter la rapidité de l'algorithme en remplaçant r_{i+1} par $\min(r_{i+1}, r_i - r_{i+1})$ en effet $p\gcd(r_i, r_{i+1}) = p\gcd(r_i, r_i - r_{i+1})$

2.4 Egalité de Bezout

Théorème 5 En notant $d = a \wedge b$ on a $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

en effet $a\mathbb{Z} + b\mathbb{Z}$ est un sous groupe additif de $\mathbb{Z}$, il est donc de la forme $d\mathbb{Z}$ pour un entier $d \in \mathbb{N}$ et cet entier est le pgcd $a \wedge b$.

Proposition 6 Soit $d = a \wedge b$, il existe $(x, y) \in \mathbb{Z}^2$ (qui ne sont pas uniques) tels que $ax + by = d$ ces entiers x et y sont appelés coefficients de Bezout de a et b.

Proposition 7 Les diviseurs communs à a et à b sont les diviseurs de d.

Propriété 4 Soit $k \in \mathbb{N}^*$, on a $(ka) \wedge (kb) = k(a \wedge b)$.

Exemple 3 coefficients de Bezout de $a = 18480$ et de $b = 9828$.

a=b.1+8652	b=8652.1+1176	8652=1176.7+420
1176=420.0+336	420=336.1+84	336=84.4

On a alors :
84=420-336=420-(1176-2.420)=3.420-1176
84=3(8652-7.1176)-1176=3.8652-22.1176
84=3.8652-22(b-8652)=25.8652-22b
84=25(a-b)-22b=25a-47b
25 et -47 sont coefficients de Bezout de a et b.

2.5 Généralisation

Théorème 8 Soit $a_1, ..., a_n$ n éléments non nuls de $\mathbb{Z}$. L'ensemble des diviseurs positifs non nuls de $a_1, ...a_n$ est un ensemble non vide majoré de $\mathbb{N}$ il admet donc un plus petit élément d appelé **plus grand commun diviseur de** $a_1, ..., a_n$ **,on note** $d = p\gcd(a_1, ..., a_n)$ **ou** $d = a_1 \wedge .... \wedge a_n$ **.**

Théorème 9 $\sum_{i=1}^{n} a_i\mathbb{Z} = d\mathbb{Z}$. Il existe donc des coefficients $(u_1.....u_n) \in \mathbb{Z}^n$ tels que $d = a_1u_1 + ... + a_nu_n$ ces coefficients sont appelés coefficients de **Bezout** .

Propriété 5 L'opération $\wedge$ est associative $a, b, c \in \mathbb{Z},\ a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Entiers premiers entre eux

Définition 3 Deux entiers relatifs a et b non nuls sont premiers entre eux si $a \wedge b = 1$, ce qui équivaut à $\mathcal{D}(a) \cap \mathcal{D}(b) = \{-1, 1\}$.

Proposition 10 Identité de Bezout.
Les entiers relatifs a et b sont premiers entre eux si et seulement si il existe $(u, v) \in \mathbb{Z}$ tel que $au + bv = 1$.

La condition est nécessaire et suffisante.

Proposition 11 si $a, b \in \mathbb{Z}^*,\ d = a \wedge b$ alors $\exists (a_1, b_1) \in \mathbb{Z}^2,\ a = da_1,\ b = db_1$ et $a_1 \wedge b_1 = 1$.

Corollaire 12 Avec les notations précédentes on a $\frac{a}{b} = \frac{a_1}{b_1}$, $\frac{a_1}{b_1}$ est la forme irréductible de $\frac{a}{b} \in \mathbb{Q}$.

Théorème 13 Théorème de Gauss.
Soient a, b, c trois entiers relatifs non nuls. Si $a \wedge b = 1$ et si $a|bc$ alors $a|c$.
$a \wedge b = 1$ et $a|bc \Longrightarrow a|c$

C'est une application de l'identité de bezout.

Proposition 14
1. $a, b, c \in \mathbb{Z}^*, (a \wedge b = 1 \text{ et } a \wedge c = 1) \Longleftrightarrow (a \wedge (bc)) = 1$.
2. $a, b_1, b_2, \cdots, b_n \in \mathbb{Z}^*,\ (\forall i \in [\![1, n]\!],\ a \wedge b_i = 1) \Longleftrightarrow (a \wedge (\prod_{i=1}^{n} b_i)) = 1$

Corollaire 15 On a l'implication :
$a \wedge b = 1 \Longrightarrow \forall (m, n) \in \mathbb{N}^2,\ a^m \wedge b^n = 1$

Définition 4 Les entiers relatifs $a_1, a_2, \cdots a_n$ sont premiers dans leur ensemble si $a_1 \wedge a_2 \wedge \cdots \wedge a_n = 1$.

Remarque 5 Des entiers premiers deux à deux sont premiers dans leur ensemble, la réciproque est fausse.
$6 \wedge 10 \wedge 15 = 1$ mais $6 \wedge 10 = 2,\ 6 \wedge 15 = 3,\ 10 \wedge 15 = 5$.

2.6 PPCM de deux ou plusieurs entiers relatifs

Définition 5 Soient a et b deux entiers relatifs. Leurs multiples communs sont $a\mathbb{Z} \cap b\mathbb{Z}$. C'est un sous groupe de $\mathbb{Z}$, il existe donc $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. m est un multiple commune de ces entiers et tou autre multiple commun est multiple de m. C'est le plus petit entier naturel strictement positif dans $a\mathbb{Z} \cap b\mathbb{Z}$. On note $m = a \vee b$.

Proposition 16 Soient $a, b \in \mathbb{Z}^*$, on a $(a \wedge b) . (a \vee b) = |a|.|b|$.

Théorème 17 Soit $a_1, ..., a_n$ n éléments non nuls de $\mathbb{Z}$. L'ensemble des multiples positifs de $a_1, ..., a_n$ est un ensemble non vide ,il admet unplus petit élément m **appelé plus petit multiple commun de** $a_1, ..., a_n$ **,on note** : $m = ppcm(a_1, ..., a_n)$ **ou** $m = a_1 \vee .... \vee a_n$

Théorème 18 $\cap_{i=1}^{n} a_i\mathbb{Z} = m\mathbb{Z}$

Propriété 6 1. $\vee : (a, b) \in \mathbb{Z}^2 \to a \vee b \in \mathbb{Z}$ est une loi associative ,commutative
2. $ppcm(\lambda a_1, ..., \lambda a_n) = |\lambda| \, ppcm(a_1, ..., a_n)$
3. $a \vee b = |b| \Longleftrightarrow a \,|b$

3 Nombres premiers

Définition 6 On appelle **nombre premier** tout entier naturel p$\geq$ 2 dont les seuls diviseurs dans $\mathbb{N}$ sont 1 et p. (Les seuls diviseurs dans $\mathbb{Z}$ sont $-p, -1, 1, p$)

Propriété 7 Un nombre premier est premier avec tout élément de $\mathbb{Z}$ qu'il ne divise pas, en particulier deux nombres premiers distincts sont premier entre eux.

Théorème 19 Tout entier $n \geq 2$ admet au moins un diviseur premier.

Théorème 20 L'ensemble des nombres premiers est infini.

Théorème 21 Tout entier $n \geq 2$ s'écrit comme produit d'un nombre fini de nombres premiers.

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} \quad p_i \ premiers \quad 2\,à\,2\,distincts$$

Cette décomposition est unique à l'ordre des facteurs près.

Proposition 22 Soit p un nombre premier $\forall k \in [\![1, p-1]\!]$, $\binom{p}{k}$ est divisible par p.

Théorème 23

$$a = \prod_{i=1}^{n} p_i^{\alpha_i} \ \ et \ \ b = \prod_{i=1}^{n} p_i^{\beta_i} \quad \Rightarrow \quad p\,\gcd(a,b) = \prod_{i=1}^{n} p_i^{\inf(\alpha_i,\beta_i)} \ \ et \ \ ppcm = \prod_{i=1}^{n} p_i^{\sup(\alpha_i,\beta_i)}$$

Les α_i ou les β_i peuvent éventuellement être nuls.

4 L'anneau $\mathbb{Z}/n\mathbb{Z}$ n$\in \mathbb{N}^*$

Rappels

4.1 Relation d'équivalence :

Définition 7 Une relation R sur un ensemble E est une relation d'équivalence si elle est réflexive,symétrique et transitive.

Proposition 24 Soit R une relation d'équivalence sur un ensemble E. Soit x un élément de E , on appelle **classe d'équivalence de x** l'ensemble des éléments de E qui sont reliés à x et on note $\overline{x}$. L'ensemble des classes d'équivalences forme une partition c'est à dire la réunion de toutes les classes d'équivalence fait E et deux classes distinctes ont une intersection vide.

Définition 8 L'ensemble des classes d'équivalence est appelé ensemble quotient et est noté E/R.

4.2 Congruence

Définition 9 Soit $n \in \mathbb{N}^*$ on définit sur $\mathbb{Z}$ la relation de congruence modulo n par

$$x \equiv y \ [n] \Longleftrightarrow x - y \in n\mathbb{Z}$$

Proposition 25 La relation de congruence est une relation d'équivalence .$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$. On dit que 0,1,...,n-1 sont les représentants canoniques des classes modulo n.

4.3 l'anneau $\mathbb{Z}/n\mathbb{Z}$

Théorème 26 La relation de congruence modulo n est compatible avec l'addition et avec la multiplication c'est à dire :

$$x \equiv y\ [n]\ \ et\ \ x' \equiv y'\ [n] \Longrightarrow x + x' \equiv y + y'\ [n]\ \ et\ xx' \equiv yy'\ [n]$$

Définition 10 On peut définir sur $\mathbb{Z}/n\mathbb{Z}$ une loi + et une loi .par $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x}.\overline{y} = \overline{x.y}$.$(\mathbb{Z}/n\mathbb{Z}, +, .)$ est un anneau commutatif.

Remarque 6 1) $\overline{0}$ est l'élément neutre pour + et $\overline{1}$ est lélément neutre pour .
2) l'application $x \in \mathbb{Z} \rightarrow \overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est un homomorphisme d'anneaux ,surjectif, de noyau $n\mathbb{Z}$.
3) $\forall k \in \mathbb{Z}\ \forall a \in \mathbb{Z} \qquad k\overline{a} = \overline{ka}$

Théorème 27 Soit n un entier supérieur à 2 et soit $a \in \mathbb{Z}$

$$\overline{a}\ \ est\ \ \ inversible\ \ dans\ \ (\mathbb{Z}/n\mathbb{Z}, \times) \Leftrightarrow a \wedge n = 1$$

L'ensemble des éléments inversibles est un groupe d'ordre $\phi(n)$, la fonction ϕ est appelée indicadrice d'Euler.

Théorème 28 Soit $p \in \mathbb{N}\backslash\{0,1\}$ .Les propriétés sont équivalentes :
1) p est premier 2) l'anneau $\mathbb{Z}/p\mathbb{Z}$ est intègre 3)l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un **corps** c'est à dire tout élément non nul a un symétrique pour la loi .