ARITHMÉTIQUE DANS Z

1. NOTIONS ÉLÉMENTAIRES

1.1. Sous-groupe de Z

THÉORÈME 1.1.0.1. —
Tout sous-groupe de $\mathbf{Z}$ est de la forme $a\mathbf{Z}$ avec $a \in \mathbf{Z}$.

DÉMONSTRATION 1.1.0.1. —
Soit G un sous-groupe de $\mathbf{Z}$. Si G est réduit à $\{0\}$ alors $G = 0\mathbf{Z}$.
Sinon, soit $x = |x| \in G$ l'élément minimal de G non nul (qui existe puisque $G \subset \mathbf{Z}$).
$x\mathbf{Z} \subset G$ puisque G est un groupe.
Soit $y \in G$. Par division euclidienne, il existe un unique couple $(a, b) \in \mathbf{Z} \times \{0, 1, \ldots, x-1\}$ tel que $y = ax + b$. On a $y - ax \in G$ mais aussi $y - ax = b \in G$.
Or $b < x$ donc $b = 0$ et donc $y \in x\mathbf{Z}$.

On notera $x\mathbf{Z} = \boldsymbol{x}$.

1.2. pgcd et ppcm

DÉFINITION 1.2.0.1. —
Soient $a, b \in \mathbf{Z}$. On dit de manière équivalente que « *a divise b* » ou :

$$a \mid b \iff \boldsymbol{b} \subset \boldsymbol{a} \iff \exists c \in \mathbf{Z}, a = cb.$$

DÉFINITION 1.2.0.2. —
Soient $a, b \in \mathbf{Z}$.
On a que $\boldsymbol{a}+\boldsymbol{b}$ est un sous-groupe de $\mathbf{Z}$ de la forme $\boldsymbol{d}$ avec $d \in \mathbf{Z}$. On note $\text{pgcd}(a, b) = d$.
$\boldsymbol{a} \cap \boldsymbol{b}$ est un sous-groupe de $\mathbf{Z}$ de la forme $\boldsymbol{m}$ avec $m \in \mathbf{N}$. On note $\text{ppcm}(a, b) = m$.

Proposition 1.2.0.1. —
Soient $a, b \in \mathbf{Z}$. On a les propositions suivantes :

1. $\text{pgcd}(a,b) = d \iff (\forall x \in \mathbf{Z}, x \mid a \text{ et } x \mid b \iff x \mid d)$;
2. $\text{ppcm}(a,b) = m \iff (\forall x \in \mathbf{Z}, a \mid x \text{ et } b \mid x \iff m \mid x)$.

Démonstration 1.2.0.2. —
Soient $a, b \in \mathbf{Z}$.

1. Soit $x \in \mathbf{Z}$. $x \mid a$ et $x \mid b \iff \boldsymbol{a} \subset \boldsymbol{x}$ et $\boldsymbol{b} \subset \boldsymbol{x} \iff \boldsymbol{a} + \boldsymbol{b} \subset \boldsymbol{x} \iff x \mid \text{pgcd}(a,b)$.
2. Soit $x \in \mathbf{Z}$. $a \mid x$ et $b \mid x \iff \boldsymbol{x} \subset \boldsymbol{a}$ et $\boldsymbol{x} \subset \boldsymbol{b} \iff \boldsymbol{x} \subset \boldsymbol{a} \cap \boldsymbol{b} \iff \text{ppcm}(a,b) \mid x$.

Théorème 1.2.0.2 (Identité de Bezout). —
Si $a, b \in \mathbf{Z}$ alors il existe $u, v \in \mathbf{Z}$ tels que $au + bv = \text{pgcd}(a,b)$.
En particulier, si a et b sont premiers entre eux alors $au + bv = 1$.

2. NOTIONS MODULAIRES

2.1. Passage au quotient

Définition 2.1.0.3. —
Soit $a \in \mathbf{Z}$, $\mathbf{Z}/\boldsymbol{a}$ est le sous-ensemble de $\mathbf{Z}$ obtenu par le quotient de $\mathbf{Z}$ par $\boldsymbol{a}$.
Si $x \in \mathbf{Z}$ alors $\overline{x}$ est la classe d'équivalence de x dans $\mathbf{Z}/\boldsymbol{a}$.

Si $\bar{x} = \bar{y} \in \mathbf{Z}/\boldsymbol{a}$ alors pour x, y des représentants de leurs classes respectives :

$$x = y + ua$$

avec $u \in \mathbf{Z}$. Il arrive de le noter :

$$x \equiv y \mod a.$$

Proposition 2.1.0.2. —
Soit $a \in \mathbf{N}$, $\mathbf{Z}/\boldsymbol{a} = \{\overline{0}, \overline{1}, \ldots, \overline{a-1}\}$.

On étend naturellement les opérations sur $\mathbf{Z}$ à $\mathbf{Z}/\boldsymbol{a}$ en identifiant les opérations de $\mathbf{Z}$ à $\mathbf{Z}/\boldsymbol{a}$. On pourra alors confondre x et son représentant $\overline{x}$ dans $\mathbf{Z}/\boldsymbol{a}$.

Proposition 2.1.0.3. —
Soient $x, y \in \mathbf{Z}$:

1. $\overline{x+y} = \overline{x} + \overline{y}$;
2. $\overline{xy} = \overline{x} \cdot \overline{y}$.

Démonstration 2.1.0.3. —
Soient $x, y \in \mathbf{Z}$.

1. si $x = ua + b$ et $y = va + c$ tels que dans les divisions euclidiennes respectives alors
$$\overline{x+y} = \overline{(u+v)a+b+c} = \overline{b+c} = \overline{b} + \overline{c} = \overline{x} + \overline{y};$$
2. de même :
$$\overline{xy} = \overline{(ua+b)(va+c)} = \overline{a(uva+uc+bv)+bc} = \overline{bc} = \overline{b} \cdot \overline{c} = \overline{x} \cdot \overline{y}.$$

2.2. Inverse modulaire

Définition 2.2.0.4. —
L'inverse par la multiplication modulo $n \in \mathbf{Z}$ d'un entier $a \in \mathbf{Z}$ est un entier $u \in \mathbf{Z}$ satisfaisant à
$$a^{-1} \equiv u \mod n.$$
C'est-à-dire de manière équivalente :
$$au \equiv 1 \mod n.$$

Proposition 2.2.0.4. —
$a \in \mathbf{Z}$ est inversible dans $\mathbf{Z}/\boldsymbol{n}$ si, et seulement si, n est premier avec a.

Démonstration 2.2.0.4. —
Soient $a, u, n, m \in \mathbf{Z}$.
$$au \equiv 1 \mod n \iff au = 1 + mn \iff au - mn = 1$$
ce qui revient à dire que $\text{pgcd}(a, n) = 1$.

Théorème 2.2.0.3. —
$\mathbf{Z}/\boldsymbol{p}$ est un corps si, et seulement si, p est premier.

Démonstration 2.2.0.5. —
$\mathbf{Z}/\boldsymbol{p}$ est un anneau. Or $x \in \mathbf{Z}/\boldsymbol{p}$ est inversible si x est premier avec p et donc tout x est inversible si p est premier.

2.3. Petit théorème de Fermat

Théorème 2.3.0.4 (Petit théorème de Fermat). —
Soient p un nombre premier et $a \in \mathbf{Z}$. Alors :
$$a^p \equiv a \mod p.$$

Démonstration 2.3.0.6. —
On procède par récurrence sur a :

1. Pour $a = 1$ c'est vérifié.
2. Pour tout $k \in \mathbf{Z}$ on a :
$$(k+1)^p \equiv k^p + 1 \mod p.$$
En effet les coefficients binomiaux à l'exceptions des premier et dernier termes disparaissent en raison d'un facteur proportionnel à p.
3. Si la proposition est vérifiée pour $a = k$ alors pour $a = k+1$ c'est également vérifié en raison du résultat précédent :
$$(k+1)^p \equiv k^p + 1 \equiv k + 1 \mod p.$$

On peut aller plus loin en généralisant ce résultat :

Théorème 2.3.0.5 (Théorème d'Euler). —
Soit $n > 0$ et a entier premier avec n alors :
$$a^{\varphi(n)} \equiv 1 \mod n.$$

Avec bien entendu φ l'indicatrice d'Euler.
Pour démontrer ce résultat on aura besoin du théorème de Lagrange :

Théorème 2.3.0.6 (Théorème de Lagrange). —
Pour tout groupe G et tout sous-groupe H de G, l'ordre (i.e. le cardinal) de H divise l'ordre de G :
$$\sharp H \mid \sharp G.$$

Démonstration 2.3.0.7 (Théorème d'Euler). —
Le groupe $(\mathbf{Z}/\boldsymbol{n})^*$ des entiers inversibles de l'anneau $\mathbf{Z}/\boldsymbol{n}$ est constitué des classes d'entiers inversibles modulo n, i.e. premiers avec n. Il y en a exactement $\varphi(n)$ donc ce groupe est d'ordre $\varphi(n)$.
Puisque a est premier avec n, $\overline{a}$ est dans le groupe $(\mathbf{Z}/\boldsymbol{n})^*$. $\overline{a}$ a donc un ordre dans ce groupe, disons m et cet ordre divise $\varphi(n)$ tel que $mk = \varphi(n)$. On a donc :
$$a^{\varphi(n)} \equiv a^{mk} \equiv (a^m)^k \equiv 1^k \equiv 1 \mod n.$$

Démonstration 2.3.0.8 (Théorème de Lagrange). —
Le cardinal de l'ensemble G/H est appelé *indice* de H dans G et est noté $[G : H]$.

De plus, ces classes forment une partition de G et chacune d'entre elles a le même cardinal que H. On a alors :

$$\sharp G = \sharp H \times [G : H].$$