Chapitre 40

Arithmétique dans $\mathbb{Z}$.

Sommaire.

Les propositions marquées de ★ sont au programme de colles.

1 Divisibilité dans $\mathbb{Z}$

1.1 Définition et propriétés élémentaires.

Définition 1

Soit $(a,b) \in \mathbb{Z}^2$. On dit que b **divise** a ($b \mid a$) s'il existe $k \in \mathbb{Z}$ tel que $a = kb$.
On dit aussi que b est **diviseur** de a, ou que a est **multiple** de b.

Notations pour les ensembles de diviseurs et multiples de $a \in \mathbb{Z}$:

$$\mathcal{D}(a) = \{b \in \mathbb{Z} : b \mid a\} \qquad \text{et} \qquad a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}.$$

Proposition 2: Faits immédiats.

Tous les entiers divisent 0 et 1 divise tous les entiers. Ajoutons que pour $(a,b,c) \in \mathbb{Z}^3$,

1. Si b est diviseur de a et si $a \neq 0$, alors $|b| \leq |a|$.
2. $b \mid a \iff a\mathbb{Z} \subset b\mathbb{Z}$.
3. Si $c \mid a$ et $c \mid b$, alors $c \mid au + bv$, pour tous u et v dans $\mathbb{Z}$.

Preuve :

1. Supposons que $b \mid a$ et $a \neq 0$, alors $\exists k \in \mathbb{Z} \mid a = bk$ et $|a| = |b||k|$.
De plus, $k \neq 0$ car $a \neq 0$, donc $|k| \geq 1$ et $|kb| \geq |b|$, on obtient bien $|a| \geq |b|$.

2. Supposons que $b \mid a$, alors $\exists k \in \mathbb{Z} \mid a = bk$, soit $m \in a\mathbb{Z} : \exists k' \in \mathbb{Z} \mid m = ak'$ donc $m = bkk'$ donc $m \in b\mathbb{Z}$.
Supposons $a\mathbb{Z} \subset b\mathbb{Z}$, on a $a \in a\mathbb{Z}$ donc $a \in b\mathbb{Z}$ donc $b \mid a$.

3. Supposons que $c \mid a$ et $c \mid b : \exists k, k' \in \mathbb{Z} \mid a = kc,\ b = k'c$. Soient $u, v \in \mathbb{Z}$.
On a alors $au + bv = kuc + k'vc = (ku + k'v)c$ avec $ku + k'v \in \mathbb{Z}$, donc $c \mid au + bv$.

Proposition 3: Plus une relation d'ordre!

Sur $\mathbb{Z}$, la relation *divise* est réflexive, transitive, mais pas antisymétrique. On a

$$\forall (a,b) \in \mathbb{Z}^2 \quad (a \mid b \text{ et } b \mid a) \iff (a = b \text{ ou } a = -b).$$

Dans le cas où $(a \mid b)$ et $(b \mid a)$, ont dit que a et b sont **associés**.

Preuve :

$\Longleftarrow$ Trivial.
$\Longrightarrow$ Supposons que $a \mid b$ et $b \mid a$. Alors $\exists k, k' \in \mathbb{Z} \mid a = kb$ et $b = k'a$.
On a alors $b = bkk'$. Si $b = 0$, alors $a = 0$ donc $a = b$. Sinon, $kk' = 1$ donc $k = \pm 1$ et $a = \pm b$.

1.2 Division euclidienne.

Théorème 4

Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

Les entiers q et r sont appelés **quotient** et **reste** dans la division euclidienne de a par b.

Preuve :

Unicité:
Soit $(q,r) \in \mathbb{Z}^2$ et $(q',r') \in \mathbb{Z}^2$ avec $0 \leq r, r' < b$ tels que $a = bq + r$ et $a = bq' + r'$.
On a $bq' + r' = bq + r$ donc $b(q' - q) = r - r'$. De plus, $0 \leq r, r' < b$ donc $-b < -r' \leq 0$.
Ainsi, $-b < r - r' < b$ donc $-b < b(q' - q) < b$ donc $-1 < q' - q < 1$ donc $q' = q$ car $q - q' \in \mathbb{Z}$.
Donc $r - r' = b \cdot 0 = 0$ donc $(q,r) = (q',r')$.

Existence:
On pose $q = \lfloor \frac{a}{b} \rfloor$ et $r = a - bq$. On a bien $a = bq + r$.
On a $\lfloor \frac{a}{b} \rfloor \leq \frac{a}{b} < \lfloor \frac{a}{b} \rfloor + 1$ donc $q \leq \frac{a}{b} < q + 1$ donc $qb \leq a < qb + b$ donc $0 \leq a - bq < b$ donc $0 \leq r < b$.

Proposition 5

Soient a et b deux entiers relatifs.
L'entier b divise a si et seulement si le reste de la division euclidienne de a par $|b|$ est nul.

Preuve :

$\boxed{\Longleftarrow}$ Trivial.
$\boxed{\Longrightarrow}$ Par unicité du reste.

1.3 PPCM de deux entiers.

Définition 6

Soient a, b deux entiers relatifs.

1. Si a et b sont non nuls, on appelle **Plus Petit Commun Multiple** de a et b, note $a \vee b$, ou encore $\text{PPCM}(a, b)$, le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$.
2. Si a ou b vaut 0, on pose $a \vee b = 0$.

Proposition 7

Soit $(a, b) \in \mathbb{Z}^2$. Leur PPCM $a \vee b$ est l'unique entier positif m tel que

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

Preuve :

Unicité:
Soient $m, m' \in \mathbb{N}$ tels que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m'\mathbb{Z}$.
Alors $m\mathbb{Z} = m'\mathbb{Z}$ donc m et m' sont associés (et positifs) donc $m = m'$.

Existence:
On a $a\mathbb{Z}$ sous-groupe de $(\mathbb{Z}, +)$, $b\mathbb{Z}$ aussi, par intersection de groupes, $a\mathbb{Z} \cap b\mathbb{Z}$ l'est aussi.
Or les sous-groupes de $\mathbb{Z}$ sont de la forme $m\mathbb{Z}$ avec $m \in \mathbb{N}$. Donc il existe un unique $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.
Vérifions que $m = \text{PPCM}(a, b)$. Clair: m est multiple commun de a et b.
De plus, $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N} = m\mathbb{Z} \cap \mathbb{N} = \{0, m, 2m, ...\}$.
Donc si $m = 0$, $\text{PPCM}(a, b) = 0$, sinon $\text{PPCM}(a, b) = m$.

Théorème 8

Soient a et b deux entier relatifs. Leur PPCM $a \vee b$ est l'unique entier positif m tel que

1. $a \mid m$ et $b \mid m$, *le PPCM est un multiple commun.*
2. $\forall \mu \in \mathbb{Z},\ (a \mid \mu \text{ et } b \mid \mu) \Longrightarrow m \mid \mu$, *tout multiple commun est multiple du PPCM.*

Preuve :

Unicité: Soient m, m' satisfaisant 1. et 2.
On a $m \mid m'$ et $m' \mid m$, par antisymétrie sur $\mathbb{N}$, $m = m'$.

Existence: Posons $m = \text{PPCM}(a, b)$.
Il satisfait 1. par définition. Soit $\mu \in \mathbb{Z}$ un multiple commun, alors $\mu \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, donc $m \mid \mu$.

1.4 PGCD de deux entiers.

Définition 9

Soient a, b deux entiers relatifs.

1. Si a et b sont non nuls, on appelle **Plus Grand Commun Diviseur** de a et b, note $a \wedge b$, ou encore $\text{PGCD}(a, b)$, le plus grand élément positif de $\mathcal{D}(a) \cap \mathcal{D}(b)$.
2. Si $a = b = 0$, on pose $a \wedge b = 0$.

Proposition 10

$$\forall (a, b) \in \mathbb{Z}^2 \quad a \wedge b = |a| \wedge |b|$$

Preuve :

On a:

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(|a|) \cap \mathcal{D}(|b|).$$

On n'a plus qu'à passer au max.

Proposition 11

Soient a, b, c, d quatre entiers relatifs. Si $a = bc + d$, alors on a $a \wedge b = b \wedge d$.

Preuve :

Supposons que $a = bc + d$. Se convaincre que $\mathcal{D}(a, b) = \mathcal{D}(b, d)$ puis passer au max. azazzzzzzzzzzzzzzzzzzzzzzzzza xqasd

Méthode

Ce lemme est l'idée principale de l'algorithme d'Euclide, vu dans le "petit" cours d'arithmétique.
Si $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, on peut appliquer cet algorithme à $|a|$ et $|b|$ pour calculer $a \wedge b$.

Proposition 12

Soit $(a, b) \in \mathbb{Z}^2$. Notons $a\mathbb{Z} + b\mathbb{Z} = \{au + bv,\ (u, v) \in \mathbb{Z}^2\}$. C'est un sous-groupe de $\mathbb{Z}$.

Le PGCD $a \wedge b$ est l'unique entier positif d tel que

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

En particulier, il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $d = au + bv$ **(relation de Bézout)**.

Méthode : Écriture effective d'une relation de Bézout.

En *remontant* les divisions euclidiennes écrites lors de l'exécution de l'algorithme d'Euclide.

Proposition 13

$$\forall (a, b) \in \mathbb{Z}^2, \quad \forall k \in \mathbb{Z}, \quad \mathrm{PGCD}(ka, kb) = |k| \cdot \mathrm{PGCD}(a, b).$$

Théorème 14

Soient a et b ddeux entiers relatifs. Leur PGCD $a \wedge b$ est l'unique entier positif d tel que

1. $d \in \mathcal{D}(a) \cap \mathcal{D}(b)$, *(le PGCD est un diviseur commun).*
2. $\forall \delta \in \mathcal{D}(a) \cap \mathcal{D}(b) \quad \delta \mid d$ *(tous les diviseurs communs divisent le PGCD).*

Corrolaire 15

$$\forall (a, b) \in \mathbb{Z}^2 \quad \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b).$$

Proposition 16

$$\forall (a, b) \in \mathbb{Z}^2, \quad \mathrm{PGCD}(a, b) \cdot \mathrm{PPCM}(a, b) = |ab|.$$