Partie I, 1)

Théorème (division euclidienne)

Soient $a, b \in \mathbb{Z}$, $b \geq 1$. $\exists!\ (q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < b$

Preuve (a) Unicité (vu en cours)

Soient $(q,r) \in \mathbb{Z}^2$, $(q',r') \in \mathbb{Z}^2$ tels que $a = bq + r$ et $0 \leq r < b$
$a = bq' + r'$ et $0 \leq r' < b$

En soustrayant les 2 égalités, on obtient $0 = b(q-q') + (r-r')$ c'est à dire $b(q-q') = r'-r$.
donc a fortiori $|b(q-q')| = |r-r'|$. C'est à dire $b|q-q'| = |r-r'|$ (car $b \geq 0$).
Or, comme $\begin{cases} 0 \leq r < b \\ 0 \leq r' < b \end{cases}$, la distance entre r et r' est inférieure à b strictement : $|r-r'| < b$.
donc $b|q-q'| < b$, càd $|q-q'| < 1$

Comme $q, q' \in \mathbb{Z}$, nécessairement, $q - q' = 0$ et donc $q = q'$, puis aussi $r = r'$.

(b) Existence.

. Elle est fondée sur les 2 propriétés fondamentales suivantes de $\mathbb{Z}$:

. **Thm** Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.
càd : si $A \subset \mathbb{Z}$, $A \neq \emptyset$ et A majorée ($\exists x \in \mathbb{R}, \forall a \in A, x \leq a$)
Alors $\exists a_0 \in A, \forall a \in A\ a \leq a_0$

. **Lemme** $\mathbb{Z}$ est archimédien
càd : Soient $m, p \in \mathbb{Z}$, $p \geq 1$. Alors $\exists n \in \mathbb{Z}\ m \leq pn$

Preuve du lemme : 1er Cas si $m \leq 0$ alors $m < pn$ avec $n = 1$ par exemple
2e Cas si $m > 0$ alors, comme $p \geq 1$
On a aussi $p(m+1) \geq m+1 > m$
donc il suffit de prendre $n = m+1$

. Démontrons l'existence de (q,r) tel que $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$ en utilisant ces 2 propriétés.

↳ Posons $A = \{n \in \mathbb{Z}, bn \leq a\}$

* Montrons que A est non vide.

1er Cas Si $a \geq 0$ alors $0 \in A$ (ou $-1 \in A$...)
2e Cas Si $a < 0$ alors, en appliquant le lemme avec $p = b$, $m = -a$, $\exists n \in \mathbb{Z}$ tel que $-a < bn$, càd $-bn < a$
donc $-n \in A$.

* Montrons que A est majorée.

Toujours par le lemme, $\exists m \in \mathbb{Z}$ tq $a < bm$. Montrons que m majore A.
Soit $n \in A$. On a $bn \leq a < bm$ donc $bn < bm$
et donc $n < m$.
Donc $\forall n \in A$, $n < m$. Donc m est un majorant de A.

↳ Ainsi $A \neq \emptyset$ et A majorée. Donc par le thm, A admet un plus grand élément q.
$q \in A$ donc $bq \leq a$.
$q+1 \notin A$ (puisque q est le plus grand élément de A) donc $b(q+1) > a$
Ainsi $bq \leq a < b(q+1) = bq + b$ càd $0 \leq a - bq < b$
Si on pose $r = a - bq$ on a donc $0 \leq r < b$ et $a = bq + r$ □

Partie I 2)

Théorème (Sous groupes de $\mathbb{Z}$)

(a) Soit $n \in \mathbb{Z}$. Alors $n\mathbb{Z}$ est un sous groupe de $(\mathbb{Z},+)$.

(b) Soit G un sous groupe de $(\mathbb{Z},+)$. Alors $\exists n \in \mathbb{Z}$, $G = n\mathbb{Z}$.

Ainsi, tout sous groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, pour un certain $n \in \mathbb{Z}$.

Preuve $\boxed{(a)}$ (Vu en cours).

Rappelons que $n\mathbb{Z} = \{a \in \mathbb{Z},\ n|a\} = \{0, n, 2n, 3n \dots, -n, -2n, -3n \dots\}$

- $n\mathbb{Z} \subset \mathbb{Z}$
- $n\mathbb{Z} \neq \emptyset$ car par exemple $0 \in n\mathbb{Z}$ $(n|0)$
- Si $a, b \in n\mathbb{Z}$, alors $n|a$ et $n|b$ donc $n|a-b$ donc $a-b \in n\mathbb{Z}$.

Ainsi $n\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$.

$\boxed{(b)}$ Soit G un sous groupe de $\mathbb{Z}$.

On cherche $n \in \mathbb{Z}$ tel que $G = n\mathbb{Z}$.

- Recherche du "candidat" potentiel n.

1er cas Si $G = \{0\}$ alors $G = 0\mathbb{Z}$, $n = 0$! C'est terminé !

2e cas Sinon $G \neq \{0\}$

Montrons qu'il existe des éléments positifs dans G.

$G \neq \{0\}$ donc il existe $a \in G$, $a \neq 0$.

Comme $a \in G$, $-a \in G$ aussi, car G est un sous-groupe.

Alors forcément, soit a, soit $-a$ est positif !

(*) Donc $G \cap \mathbb{N}\setminus\{0\} \neq \emptyset$ (càd il existe des éléments strict^t positifs dans G)

Soit n le plus petit de ces éléments positifs strictement, dans G.

- Montrons qu'alors $G = n\mathbb{Z}$, où n est le plus petit élément positif de G.

On raisonne par double inclusion.

- Montrons que $n\mathbb{Z} \subset G$

Si $a \in n\mathbb{Z}$, $a = kn$ pour un certain $k \in \mathbb{Z}$

Alors $a = \underbrace{n+n+\dots+n}_{k \text{ fois}}$. Or $n \in G$. Donc $n+n \in G$, $n+n+n \in G \dots$ et ainsi $a \in G$. (car G est un sous groupe)

donc $\forall a \in n\mathbb{Z}$, $a \in G$ et ainsi $n\mathbb{Z} \subset G$

- Montrons que $G \subset n\mathbb{Z}$

Soit $a \in G$. Ecrivons la division euclidienne de a par n :

$\exists!\,(q,r) \in \mathbb{Z}^2$, $a = qn + r$ et $0 \leq r < n$

ainsi $r = a - qn$ avec $a \in G$, $qn \in n\mathbb{Z} \subset G$.

donc, comme G est un sous groupe, $r \in G$

or $r \geq 0$ et $r < n$, et n est le plus petit élément de G strictement positif.

donc $r = 0$.

donc $a = qn \in n\mathbb{Z}$, et ainsi

$\forall a \in G$, $a \in n\mathbb{Z}$. Donc $G \subset n\mathbb{Z}$.

Finalement $G \subset n\mathbb{Z}$, $n\mathbb{Z} \subset G$ et ainsi $G = n\mathbb{Z}$. □

(*) On utilise la version suivante du Thm donnant la propriété fondamentale de $\mathbb{Z}$:

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

(ici $G \cap \mathbb{N}\setminus\{0\}$ est non vide, minorée par 0)

Partie II 1)

Théorème et Définition (PGCD de 2 entiers).

Soient $a, b \in \mathbb{Z}^*\setminus\{0\}$.

1) $\exists!\, d \in \mathbb{N}^*\setminus\{0\}$, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

2) $\exists\,(u,v) \in \mathbb{Z}^2$, $d = au + bv$. (identité de Bézout)

3) - $d|a$ et $d|b$.

- Si $d'|a$ et $d'|b$ alors $d'|d$. $(d' \in \mathbb{N})$

Ainsi d est le plus grand diviseur commun à a et b.

On l'appelle PGCD (a,b) et on le note $d = a \wedge b$.

Preuve $\boxed{1)}$. $a\mathbb{Z} + b\mathbb{Z} \neq \emptyset$ car $0 = a \times 0 + b \times 0 \in a\mathbb{Z} + b\mathbb{Z}$.

- $a\mathbb{Z} + b\mathbb{Z} \subset \mathbb{Z}$.
- Si $x, x' \in a\mathbb{Z} + b\mathbb{Z}$ Alors $x = ak + b\ell$, $k, \ell \in \mathbb{Z}$; $x' = ak' + b\ell'$, $k', \ell' \in \mathbb{Z}$ donc $x - x' = a\underbrace{(k-k')}_{\in \mathbb{Z}} + b\underbrace{(\ell-\ell')}_{\in \mathbb{Z}} \in a\mathbb{Z} + b\mathbb{Z}$

donc $a\mathbb{Z} + b\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$. Donc par thm précédent, $\exists d \in \mathbb{N}^*\setminus\{0\}$ $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$

$\boxed{2)}$ $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ donc il existe $(u,v) \in \mathbb{Z}^2$, $d = au + bv$.

$\boxed{3)}$. $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \Rightarrow \begin{cases} a\mathbb{Z} \subset d\mathbb{Z} \\ b\mathbb{Z} \subset d\mathbb{Z} \end{cases} \Rightarrow \begin{cases} d|a \\ d|b \end{cases}$

. Si $d'|a$ et $d'|b$,

On écrit $d = au + bv$ par 2). Alors $d'|d = au + bv$. □