$\mathbb{N} = \{0; 1; 2; 3; \dots\}$

inclus

Axiome : Si $E \subset \mathbb{N}$ (E est une partie de n.)
$E \neq \emptyset$

$\exists\, x \in E$ tq. $x \leq y$ $\forall\, y \in E$

il existe — tel que — pour tout

$\boxed{a \in \mathbb{Z},\ b > 0}$ b entier

a	b
-15	3
82	17
-1000	1
100	23

Prop. $\exists\, q \in \mathbb{Z}$ et $0 \leq r < b$,
r entier, tq.

$$\boxed{a = b \cdot q + r}$$

82	17
68	4
14	

$$\underset{a}{82} = \underset{b}{17} \cdot \underset{q}{4} + \underset{r}{14}$$

4.2.1

d) $\boxed{(a \mid b \text{ et } a \mid c)} \Rightarrow a \mid (b+c)$

Connu

preuve: $a \mid b \Rightarrow b = z_1 \cdot a$ pour $z_1 \in \mathbb{Z}$

$a \mid c \Rightarrow c = z_2 \cdot a$ pour $z_2 \in \mathbb{Z}$

$$\left.\begin{array}{l} b = z_1 \cdot a \\ c = z_2 \cdot a \end{array}\right\} \Rightarrow b+c = z_1 a + z_2 a \Rightarrow b+c = (z_1+z_2) \cdot a$$

Or, $\boxed{z_1 + z_2 \in \mathbb{Z}}$ si $z_1, z_2 \in \mathbb{Z}$

$\Rightarrow b+c = w \cdot a$ avec $w = z_1 + z_2 \in \mathbb{Z}$

$\Rightarrow a \mid (b+c)$

$x = 17 + 26 \cdot k \quad k \in \mathbb{Z}$

$$\begin{array}{c|l} x & 26 \\ \cline{2-2} & k \\ \hline 17 & \end{array}$$

$$\boxed{\mathbb{Z}_{26}} = \mathbb{Z}/_{26\mathbb{Z}} = \{0; 1; 2; \dots ; 24; 25\}$$

1932458762 19

Σ_i : $9+2+5+7+2+9 = 34$

$34 - 23 = 11$

Σ_p : 23

5432112345 mod 11123

modulo : reste après division par
(% python)

$$a = b \cdot q + r$$

$$\frac{a}{b} = q + \boxed{\frac{r}{b}} \quad \Big\downarrow -q$$

$$\frac{a}{b} - q = \frac{r}{b} \quad \Big\downarrow \cdot b$$

$$a - qb = r \checkmark$$

$\mathbb{Z}_3 = \{0; 1; 2\}$

$0 + k \cdot 3 \qquad k = 0, 1, -1, 2, -2$

$-9, -6, -3, 0, 3, 6, 9$

$a \mid b \Rightarrow \exists z \in \mathbb{Z}$ tq. $b = a \cdot z$ | hypothèse

---

hypothèse $\rightarrow$ conclusion

Etape 1

Etape 2

⋮

Utilisation de la déf.

4.2.1

a) hyp. $a \in \mathbb{Z}$

concl. $a \mid a$

preuve: $a \in \mathbb{Z} \Rightarrow a = \underset{\in \mathbb{Z}}{1} \cdot a \Rightarrow \exists z \in \mathbb{Z}$ tq. $a = z \cdot a$
$\Leftrightarrow a = a \cdot z$

$\Rightarrow a \mid a \quad \square$

Connu : $a, b \in \mathbb{Z}$ $\quad a|b$ et $b|a \Rightarrow a = \pm b$

$\boxed{a \in \mathbb{Z} \text{ tq. } a|1}$

On sait de plus que $1|a$.

Donc $a|1$ et $1|a$

Donc $\boxed{a = \pm 1}$

$a|a \quad \forall a \in \mathbb{Z}$

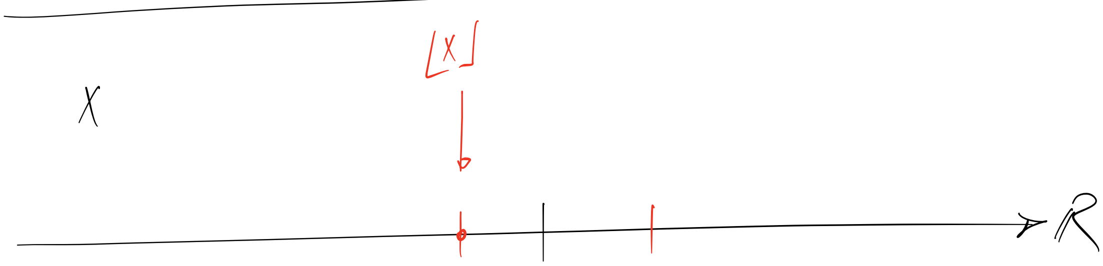
donné $\quad$ connu $\quad$ connu

$\boxed{a \in \mathbb{Z}}$ $\boxed{1 \in \mathbb{Z}}$ $\boxed{a = a \cdot 1}$

preuve: $a \in \mathbb{Z}$ $\quad$ $\boxed{\text{On sait que } 1 \in \mathbb{Z} \text{ et que } a = a \cdot 1}$

$\Rightarrow \boxed{\exists z \in \mathbb{Z} \text{ tq. } a = a \cdot z}$

$\Rightarrow a|a$



$m < x < m+1$