Arithmétique

Arithmétique

Divisibilité

Soit $a, b \in \mathbb{Z}$

a divise b / b multiple de a

$$\exists k \in \mathbb{Z} \qquad ak = b$$

Notations

- $a \mid b$ pour « a divise b »
- $a \nmid b$ pour « a ne divise pas b »

Exemples

- $2 \mid 4$ car $2 \times 2 = 4$
- $3 \mid 12$ car $3 \times 4 = 12$
- $3 \nmid 14$ car on n'a jamais $3 \times k = 14$ avec $k \in \mathbb{Z}$

Arithmétique

Divisibilité

Ensemble des diviseurs positifs

$$\mathcal{D}(a) = \{d \in \mathbb{N} \mid d \text{ divise } a\}$$

Exemples

- $\mathcal{D}(12) = \{1, 2, 3, 4, 6, 12\}$
- $\mathcal{D}(-12) = \{1, 2, 3, 4, 6, 12\}$
- $\mathcal{D}(14) = \{1, 2, 7, 14\}$
- $\mathcal{D}(97) = \{1, 97\}$
- $\mathcal{D}(1) = \{1\}$
- $\mathcal{D}(0) = \mathbb{N}$

Arithmétique

Divisibilité

Ensemble des multiples positifs

$$\mathcal{M}(a) = \{m \in \mathbb{N} \mid a \text{ divise } m\}$$

Exemples

- $\mathcal{M}(12) = \{0, 12, 24, 36, 48, 60, \ldots\}$
- $\mathcal{M}(-12) = \{0, 12, 24, 36, 48, 60, \ldots\}$
- $\mathcal{M}(14) = \{0, 14, 28, 42, 56, 70, \ldots\}$
- $\mathcal{M}(97) = \{0, 97, 194, 291, 388, 485, \ldots\}$
- $\mathcal{M}(1) = \mathbb{N}$
- $\mathcal{M}(0) = \{0\}$

Arithmétique

Divisibilité

Propriétés

Soit $a, b, c, m, n \in \mathbb{Z}$.

1. $a \mid 0$
2. $1 \mid a$

3. si $a \mid b$ et $b \neq 0$ alors $|a| \leq |b|$
4. $\mathcal{D}(a)$ est fini si et seulement si $a \neq 0$
5. $\mathcal{M}(a)$ est fini si et seulement si $a = 0$

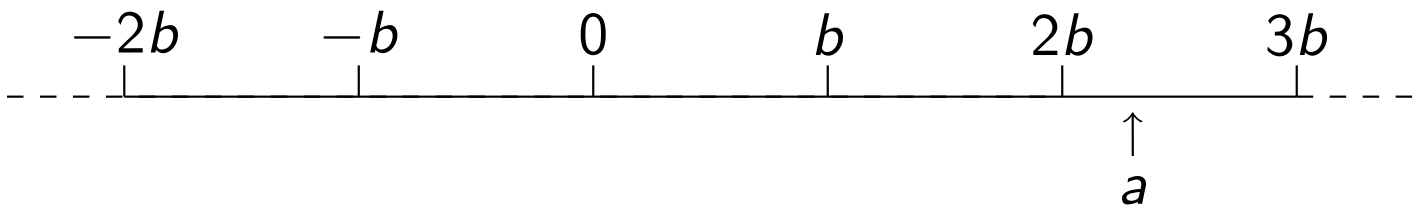
6. $a \mid a$
7. $a \mid b$ et $b \mid c \quad \Rightarrow \quad a \mid c$
8. $a \mid b$ et $b \mid a \quad \Rightarrow \quad |a| = |b|$

9. $c \mid a$ et $c \mid b \quad \Rightarrow \quad c \mid ma + nb$

Division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.
Il existe un unique $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$

Illustration pour $b > 0$



d'où

$$qb \leq a < (q+1)b$$

donc

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

Arithmétique

Division euclidienne

Division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.
Il existe un unique $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$

Notations

- $a \operatorname{div} b$ pour le quotient q
- $a \bmod b$ pour le reste r

Exemples

- $46 = 5 \times 9 + 1$ donc $46 \operatorname{div} 5 = 9$, $46 \bmod 5 = 1$
- $46 = 8 \times 5 + 6$ donc $46 \operatorname{div} 8 = 5$, $46 \bmod 8 = 6$
- $46 = -8 \times -5 + 6$ donc $46 \operatorname{div} -8 = -5$, $46 \bmod -8 = 6$
- $-46 = 8 \times -6 + 2$ donc $-46 \operatorname{div} 8 = -6$, $-46 \bmod 8 = 2$
- $-46 = -8 \times 6 + 2$ donc $-46 \operatorname{div} -8 = 6$, $-46 \bmod -8 = 2$

Division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.
Il existe un unique $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$

Preuve (existence)

D'abord pour $(a, b) \in \mathbb{N} \times \mathbb{N}^*$

```
1 Fonction divmod(a, b : entiers) :
2     (q,r) ← (0,a)
3     tant que r ≥ b faire
4         r ← r - b
5         q ← q + 1
6     retourner (q,r)
```

- invariant : à chaque tour de boucle $a = bq + r$
- terminaison : $r - b$ décroit strictement car $b > 0$
- conclusion : à la fin $a = bq + r$ et $0 \leq r < b$

Division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.
Il existe un unique $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$

Preuve (existence)

Puis pour $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$:

- si $a \geq 0$ et $b > 0$: $\text{divmod}(a, b) = (q, r)$ convient
- si $a \geq 0$ et $b < 0$:
  $\text{divmod}(a, -b) = (q, r)$ avec $a = -bq + r$ et $0 \leq r < -b$

  donc $(q', r') = (-q, r)$ convient

Arithmétique

Division euclidienne

Division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.

Il existe un unique $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$

Preuve (existence)

Puis pour $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$:

- si $a < 0$ et $b > 0$:
  divmod$(-a, b) = (q, r)$ avec $-a = bq + r$ et $0 \leq r < b$
  - si $r = 0$: alors $(q', r') = (-q, r)$ convient
  - si $r > 0$: alors $(q', r') = (-q - 1, b - r)$ convient car

$$bq' + r' = b(-q - 1) + b - r = -bq - r = a$$

et

$$0 \geq -r > -b \text{ donc } b \geq b - r > 0$$

Division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.
Il existe un unique $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$

Preuve (existence)

Puis pour $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$:

- si $a < 0$ et $b < 0$:
  divmod$(-a, -b) = (q, r)$ avec $-a = -bq + r$ et $0 \leq r < -b$
  - si $r = 0$: alors $(q', r') = (q, r)$ convient
  - si $r > 0$: alors $(q', r') = (q + 1, -b - r)$ convient car

$$bq' + r' = b(q + 1) - b - r = bq - r = a$$

et

$$0 \geq -r > b \text{ donc } -b \geq -b - r > 0$$

Arithmétique

Division euclidienne

Division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.
Il existe un unique $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$

Preuve (unicité)

Soit $(q, r), (q', r') \in \mathbb{Z}^2$ tels que

$$\begin{array}{l} a = bq + r \\ a = bq' + r' \end{array} \quad \text{et} \quad \begin{array}{l} 0 \leq r < |b| \\ 0 \leq r' < |b| \end{array}$$

Alors $$-|b| < r - r' < |b|$$

et

$$bq + r = bq' + r' \qquad \text{d'où} \qquad b(q - q') = r' - r$$

Comme $r' - r$ multiple de b entre $-|b|$ et $|b|$ nécessairement $r' - r = 0$ et par suite puisque $b \neq 0$ alors $q - q' = 0$ □

Arithmétique

Arithmétique modulaire et congruences

Propriétés

Soit $a, b \in \mathbb{Z}, c \in \mathbb{Z}^*$ et $n \in \mathbb{N}^*$.

1. $(a + b) \bmod c = ((a \bmod c) + (b \bmod c)) \bmod c$
2. $(a \times b) \bmod c = ((a \bmod c) \times (b \bmod c)) \bmod c$
3. $(a \bmod c) \bmod c = a \bmod c$
4. $a^n \bmod c = (a \bmod c)^n \bmod c$

Exemples

- $(79 + 68) \bmod 49 = (30 + 19) \bmod 49 = 49 \bmod 49 = 0$
- $(79 \times 68) \bmod 49 = (30 \times 19) \bmod 49 = (10 \times 3 \times 19) \bmod 49 = (10 \times 57) \bmod 49 = (10 \times 8) \bmod 49 = 80 \bmod 49 = 31$
- $2^{12} \bmod 49 = (2^6)^2 \bmod 49 = 64^2 \bmod 49 = 15^2 \bmod 49 = (3 \times 75) \bmod 49 = (3 \times 26) \bmod 49 = 29$

Arithmétique

Arithmétique modulaire et congruences

Soit $m \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$.

Congruence

$$a \equiv_m b \quad :\Leftrightarrow \quad m \mid a - b$$

Autres notations

$$a \equiv b \mod m \qquad \text{ou aussi} \qquad a \equiv b \ [m]$$

Exemples

- $46 \equiv_5 1$
- $46 \equiv_8 6$
- $-46 \equiv_8 2$
- $46 \equiv_5 26$
- $46 \equiv_5 -19$
- $45 \equiv_5 0$

Propriétés

Soit $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$.

1. $a \equiv_m a$
2. $a \equiv_m b \quad \Rightarrow \quad b \equiv_m a$
3. $a \equiv_m b$ et $b \equiv_m c \quad \Rightarrow \quad a \equiv_m c$

4. $a \equiv_m b$ et $c \equiv_m d \quad \Rightarrow \quad a + c \equiv_m b + d$
5. $a \equiv_m b$ et $c \equiv_m d \quad \Rightarrow \quad a \times c \equiv_m b \times d$
6. $a \equiv_m b \quad \Rightarrow \quad a^n \equiv_m b^n$

7. $a \equiv_m b \quad \Leftrightarrow \quad a \bmod m = b \bmod m$

Arithmétique

Arithmétique modulaire et congruences

Exemples

- $79 + 68 \equiv_{49} 30 + 19 \equiv_{49} 49 \equiv_{49} 0$
- $79 \times 68 \equiv_{49} 30 \times 19 \equiv_{49} 10 \times 57 \equiv_{49} 10 \times 8 \equiv_{49} 31$
- $2^{12} \equiv_{49} (2^6)^2 \equiv_{49} 64^2 \equiv_{49} 15^2 \equiv_{49} 3 \times 75 \equiv_{49} 3 \times 26 \equiv_{49} 29$

Attention

$\equiv_m$ n'est pas compatible en général avec la simplification :

$$2 \times 3 \equiv_6 4 \times 3 \qquad \text{mais} \qquad 2 \not\equiv_6 4$$

ni avec des puissances congrus :

$$4 \equiv_5 9 \quad \text{mais} \quad 2^4 \not\equiv_5 2^9$$