Divisibilité dans $\mathbb{Z}$ $\mathbb{N}$ désigne l'ensemble des entiers naturels $\{0, 1, 2, ...\}$
$\mathbb{Z}$ désigne l'ensemble des entiers relatifs $\{.., -2, -1, 0, 1, 2, ...\}$

Définition 1 *a et b deux entiers relatifs on dit que b divise a, ou a est un multiple de b (notation $b|a$) lorsqu'il existe $q \in \mathbb{Z}$ tel que $a = bq$*

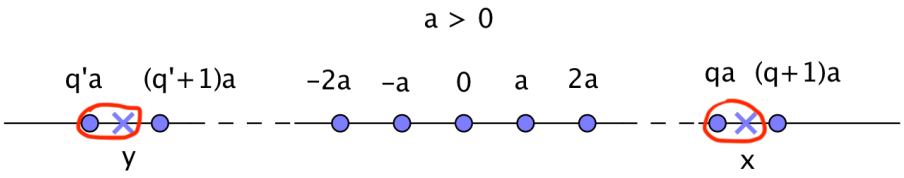
Exemples : $5|10$ car $10 = 5 \times 2$, $-5|10$ car $10 = -5 \times -2$

Théorème 1
1. $\forall x \in \mathbb{Z}$, $1|x$ *et* $x|0$
2. $0|x \iff x = 0$
3. $a|b \iff -a|b \iff a|-b$
4. $c|a$ *et* $c|b$ *entraîne que* $c|(a+b)$ *puis* $c|(a-b)$ *puis plus généralement toute* ***combinaison linéaire*** $au + bv$ *où* u *et* v *sont des entiers relatifs*
5. $\forall x, y, z \in \mathbb{Z}$ *si* $x|y$ *et* $y|z$ *alors* $x|z$ *(transitivité de la divisibilité)*
6. *Si* $a|b$ *et* $b \neq 0$ *alors* $0 \leqslant |a| \leqslant |b|$
7. *Si* $a|b$ *et* $b|a$ *alors* $a = b$ *ou* $a = -b$

Preuve :
1. $\forall x \in \mathbb{Z}$ $x = x \times 1$ et $0 = 0 \times x$
2. (a) si 0 divise un entier relatif x cela signifie qu'il existe y relatif tel que $x = 0 \times y = 0$
   (b) Réciproquement 0 divise lui-même
3. Montrons que $a|b \iff -a|b$:
   (a) Si $a|b$ alors il existe $c \in \mathbb{Z}$ tel que $b = ac$ que l'on peut réécrire $b = -a \times -c$ donc $-a|b$
   (b) La démonstration précédente prouve aussi la réciproque
4. Si $c|a$ alors $c|au$ pour tout $u \in \mathbb{Z}$ en effet il existe $k \in \mathbb{Z}$ tel que $a = kc$ donc $au = (uk)c$ ce qui signifie que $c|au$
   Si $c|a$ et $c|b$ alors $c|a+b$ en effet il existe $k \in \mathbb{Z}$ tel que $a = kc$ et il existe $l \in \mathbb{Z}$ tel que $b = lc$ donc $a + b = (k + l)c$ donc $c|a + b$

Exercice 1
Prouver le 5, 6 et 7

On note $a\mathbb{Z}$ avec $a \in \mathbb{N}$ car $2\mathbb{Z} = -2\mathbb{Z}$ l'ensemble des multiples de a



Intuitivement pour tout $a \in \mathbb{Z}$, l'ensemble $a\mathbb{Z}$ forme un **réseau** de $\mathbb{Z}$, c'est à dire un sous-ensemble de points de $a\mathbb{Z}$ régulièrement espacés et tout entier relatif sera à une distance (positive) r $<$ a d'un point unique qa du réseau
Autrement dit

Théorème 2 ***(Théorème de la division euclidienne)*** $\forall a \in \mathbb{Z}\ \forall b \in \mathbb{N}^*\ \exists\ !q \in \mathbb{Z}\ \exists\ !r \in \mathbb{N}$ *tel que* $a = bq + r$ *avec* $0 \leqslant r < b$

Preuve :

Propriété (admise) Toute partie P non vide de $\mathbb{N}$ admet un **unique** plus petit élément notée $\min(P)$

Considérons l'ensemble $E = \{a - kb \geqslant 0 | k \in \mathbb{Z}\}$ (On retranche à a les multiples de b de telle sorte que le résultat est toujours positif ou nul)

Cas $a > 0$: Vérifions que E est non vide en effet E contient au moins $a - 0 \times b = a \geqslant 0$. Puisque E est non vide d'après la propriété admise E a un plus petit élément **unique** $r \geqslant 0$ tel que $r = a - bq$ Il nous reste à prouver que

1. $0 \leqslant r < b$
2. q est unique

En effet

1. Il semble évident que le plus petit des $a - bk \geqslant 0$ soit dans l'intervalle $[0; b[$ mais démontrons le quand même si $r = a - bq \geqslant b$ alors retranchons à r une fois b on obtient $0 \leqslant r - b < r$ c'est à dire $r - b = a - bq - b = a - (q + 1)b < r$ on a donc trouvé un élément de E, $a - (q + 1)b$ strictement plus petit que r ce qui contredit le fait que r est le plus petit élément de E donc $0 \leqslant r < b$
2. q est unique car s'il existait un autre entier relatif s tel que $r = a - bq = a - bs$ alors $a - bq = a - bs$ et b(q-s) = 0 or par hypothèse $b > 0$ donc $q - s = 0$ autrement dit $q = s$

Exercice 2

Prouver le cas $a < 0$

D'où un algorithme pour $a > 0$

Algorithme 1 : division euclidienne de a par b

Données : Un entier naturel a, un entier naturel $b \geqslant 1$

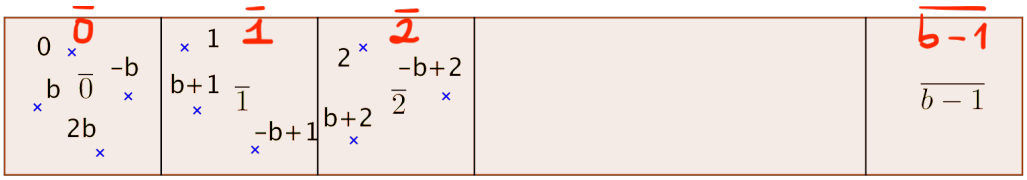
Résultat : le quotient q et le reste r tel que $a = bq + r$ avec $0 \leqslant r < b$

```
1  début
2      dividende ← a
3      diviseur ← b
4      reste ← dividende
5      quotient ← 0
6      tant que reste > diviseur faire
7          reste ← reste - diviseur
8          quotient ← quotient + 1
9      fin
10     afficher quotient
11     afficher reste
12 fin
```

Modifier l'algorithme pour $a < 0$

En Python

```
dividende = int(input("Entrez un entier naturel  a"))
diviseur   = int(input("Entrez un entier naturel  b >= 1 "))
reste = dividende
quotient = 0
while  reste > diviseur :
     reste = reste - diviseur
     quotient = quotient + 1
print("le quotient de ",dividende," par ",diviseur,\
" est ", quotient)
print(" le reste  est ",reste)
```



Partition de $\mathbb{Z}$. Congruences dans $\mathbb{Z}$ *Avoir le même reste par la division euclidienne par b partitionne $\mathbb{Z}$, c'est à dire "découpe " $\mathbb{Z}$ en b parties infinies disjointes, autant que les restes possibles par la division par b : 0,1,2,...,$b-1$*

Définition 2 *Etant donné n un entier naturel $\geqslant 2$. On dit que a et b sont congrus modulo n si a et b ont le même reste par la division par n. On note cela $a \equiv b\ [n]$. Autrement dit a et b différent d'un multiple de n, c'est à dire il existe $q \in \mathbb{Z}$ tel que $a - b = qn$ (ou encore $a = b + qn$)*

Exemples : $2020 \equiv 22 \equiv 4\ [9]$, $-34 \equiv 2\ [9]$, $1171291471001 \equiv 1171291471098[97]$

Théorème 3 *1. $\forall a \in \mathbb{Z}\ a \equiv a\ [n]$ (on dit que $\equiv$ est une relation réflexive sur $\mathbb{Z}^2$)*

2. *$\forall a \in \mathbb{Z}$ si $a \equiv b\ [n]$ alors $b \equiv a\ [n]$ (on dit que $\equiv$ est une relation symétrique sur $\mathbb{Z}^2$)*
3. *$\forall a \in \mathbb{Z}$ si $a \equiv b\ [n]$ et si $b \equiv c\ [n]$ alors $a \equiv c\ [n]$ (on dit que $\equiv$ est une relation symétrique sur $\mathbb{Z}^2$)*
4. *On note $\overline{k} = n\mathbb{Z} + k$ pour k entier tel que $0 \leqslant k \leqslant n-1$*
   $\forall x \in \overline{k}\ x \equiv k[n]$
   Les sous ensembles $\overline{k}$ pour $0 \leqslant k \leqslant n-1$ forment une partition de $\mathbb{Z}$, c'est à dire $\mathbb{Z}$ est la réunion disjointe des n sous-ensembles $\overline{k}$

Preuve :
Lorsqu'une relation R sur un ensemble E vérifient 1) 2) et 3) on dit que la relation est une **relation d'équivalence** d'ailleurs le symbole $\equiv$ signifie aussi "est équivalent à"

1. a a le même reste que lui-même
2. le "et" dans la phrase "a et b ont le même reste par la division par n" fait que la relation est symétrique

3. Evident
4. Montrons que $\mathbb{Z}$ est l'union disjointe des $\overline{k}$ (on dit que les ensembles $\overline{k}$ forment une partition de $\mathbb{Z}$
   Tout entier relatif est dans un des ensembles $\overline{k}$ d'après le théorème de la division euclidienne.
   D'après le théorème de la division euclidienne le reste est unique donc les ensembles $\overline{k}$ sont **disjoints deux à deux**

On dit que les sous ensembles $\overline{k}$ sont des **classes d'équivalence**

Exemple

Modulo 3, il y a 3 **classes d'équivalence**, les multiples de 3 notés $\overline{0}$, les multiples de 3 auxquels on rajoute 1 notés $\overline{1}$ et enfin les multiples de 3 auxquels on rajoute 2 notés $\overline{2}$

Théorème 4 *(compatibilité de $\equiv$ avec $+$ et $\times$)*

1. *si $a \equiv a'$ $[n]$ et $b \equiv b'$ $[n]$ alors $a + b \equiv a' + b'$ $[n]$*
2. *si $a \equiv a'$ $[n]$ et $b \equiv b'$ $[n]$ alors $a \times b \equiv a' \times b'$ $[n]$*
3. *si $a \equiv b$ $[n]$ alors $a^k \equiv b^k$ $[n]$ pour tout k entier*

Preuve :

1. Par hypothèse il existe $k \in \mathbb{Z}$ tel que $a - a' = kn$ et il existe $l \in \mathbb{Z}$ tel que $b - b' = ln$. Ajoutons les deux égalités terme à terme on obtient
   $a + b - (a' + b') = (k + l)n$ ce qui signifie que $a + b \equiv a' + b'$ $[n]$
2. Par hypothèse il existe $k \in \mathbb{Z}$ tel que $a = a' + kn$ et il existe $l \in \mathbb{Z}$ tel que $b = b' + ln$. Multiplions les deux égalités terme à terme on obtient
   $ab = a'b' + kn(b' + ln) + a'ln = a'b' + n(a'l + k(b' + ln))$ ce qui signifie que $a \times b \equiv a' \times b'$ $[n]$

Exercice 3

Démontrer le 3) par récurrence sur k