Arithmétique

arithmós : nombre – Dans l'antiquité, l'arithmétique était avec l'astronomie, la géométrie et la musique, une des quatre sciences mathématiques. Au Moyen-Age, ces mêmes 4 disciplines formèrent le *quadrivium*.

Chez les Pythagoricien, les relations entre les nombres entiers avaient une dimension religieuse.

L'arithmétique porte sur les **nombres entiers**.

- On se limite parfois aux positifs : $\mathbb{N}$
- On peut considérer l'ensemble des entiers, positifs ou négatifs : $\mathbb{Z}$.

I. Division euclidienne

1) Propriété

Pour a et b entiers de $\mathbb{Z}$, $b \neq 0$, il existe une unique paire entière q et r telle que :

$$a = q \cdot b + r, \quad \text{avec } 0 \leq r < |b|$$

q est le **quotient** ; r est le **reste**.

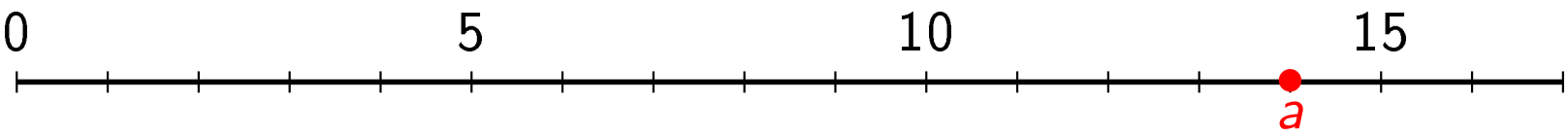
1) Propriété

Pour a et b entiers de $\mathbb{Z}$, $b \neq 0$, il existe une unique paire entière q et r telle que :

$$a = q \cdot b + r, \quad \text{avec } 0 \leq r < |b|$$

q est le **quotient** ; r est le **reste**.

Exemple : $a = 14$ et $b = 4$



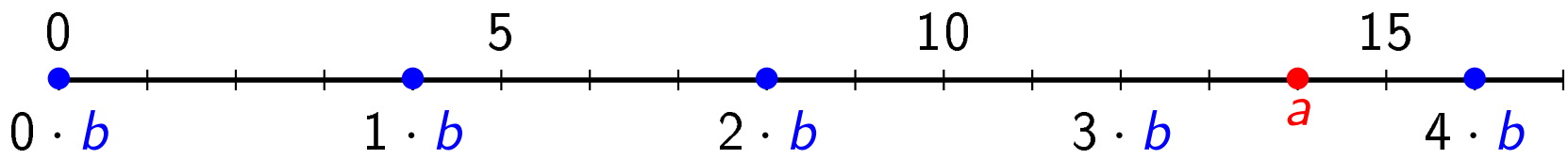
1) Propriété

Pour a et b entiers de $\mathbb{Z}$, $b \neq 0$, il existe une unique paire entière q et r telle que :

$$a = q \cdot b + r, \quad \text{avec } 0 \leq r < |b|$$

q est le **quotient** ; r est le **reste**.

Exemple : $a = 14$ et $b = 4$



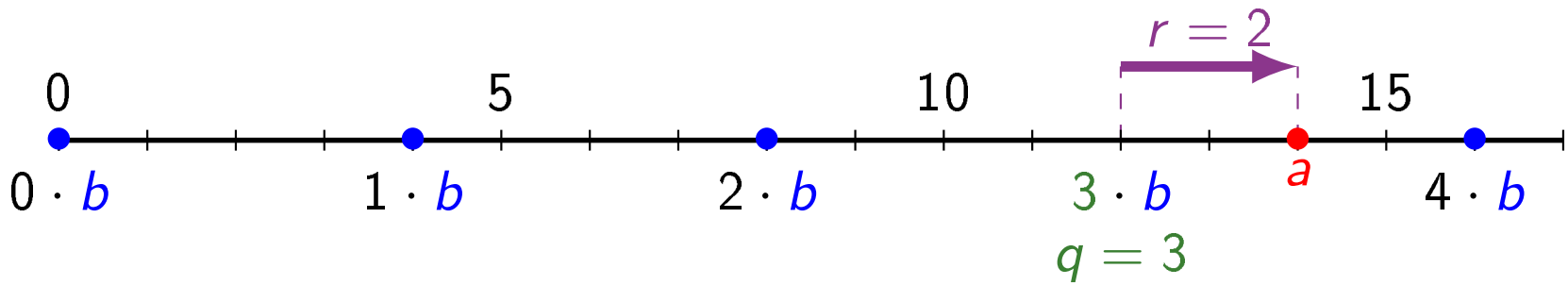
1) Propriété

Pour a et b entiers de $\mathbb{Z}$, $b \neq 0$, il existe une unique paire entière q et r telle que :

$$a = q \cdot b + r, \quad \text{avec } 0 \leq r < |b|$$

q est le **quotient** ; r est le **reste**.

Exemple : $a = 14$ et $b = 4$



$$14 = 3 \times 4 + 2$$

Exercice 1 Trouvez la paire q et r dans les cas suivants

a) $a = 15$ et $b = 4$

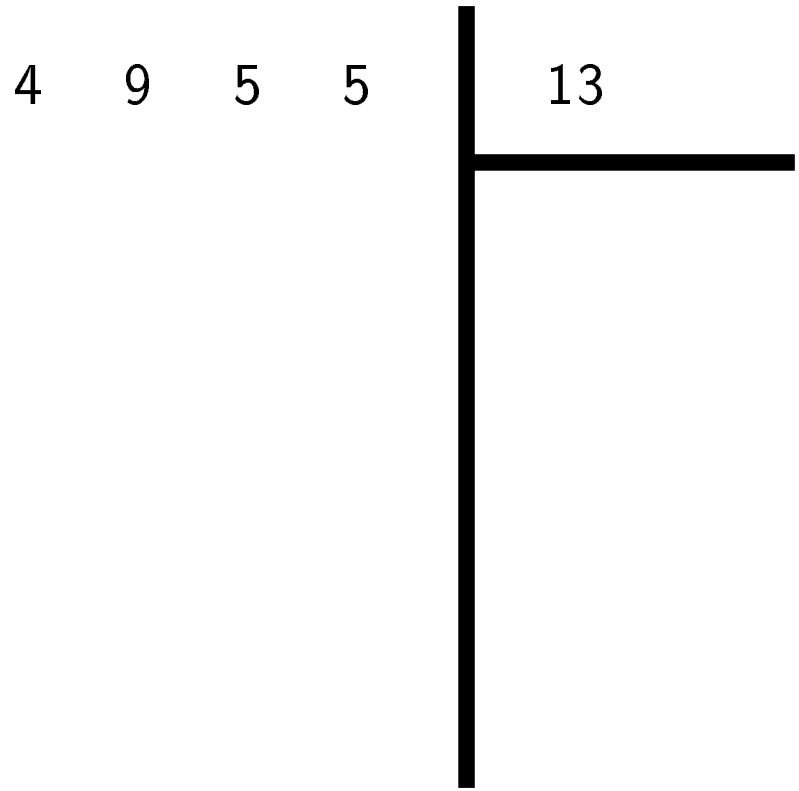
b) $a = 0$ et $b = 5$

c) $a = 15$ et $b = 17$

d) $a = -12$ et $b = 7$

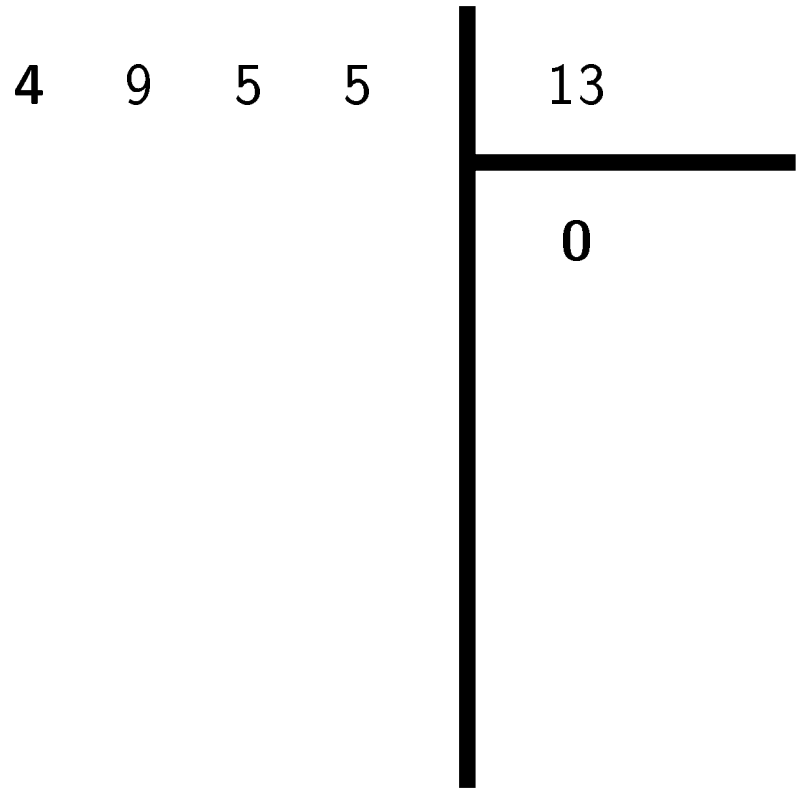
2) Algorithme du primaire

Exemple : $4955 \div 13$



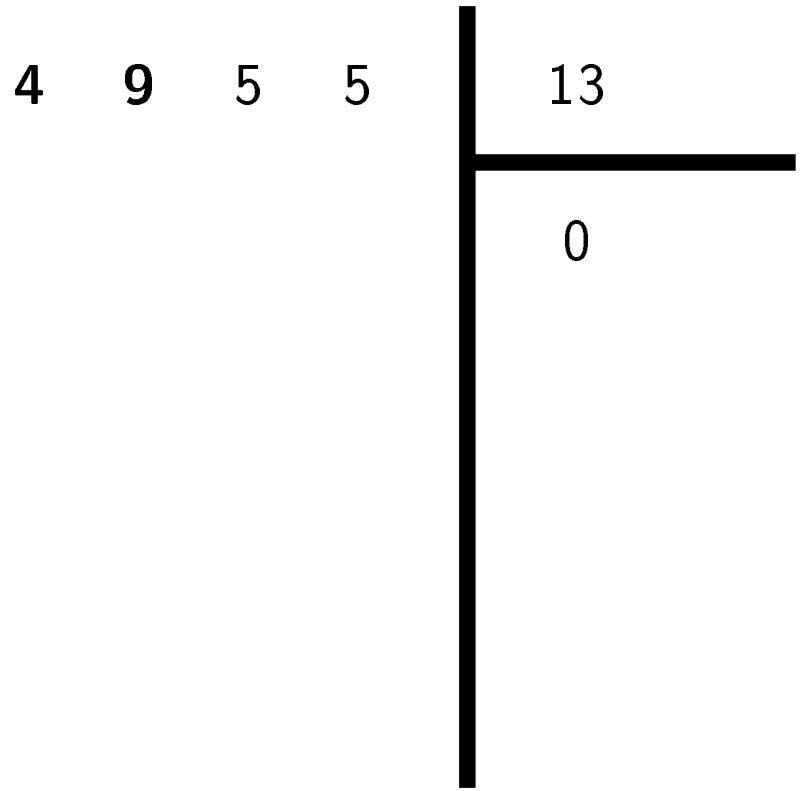
2) Algorithme du primaire

Exemple : $4955 \div 13$



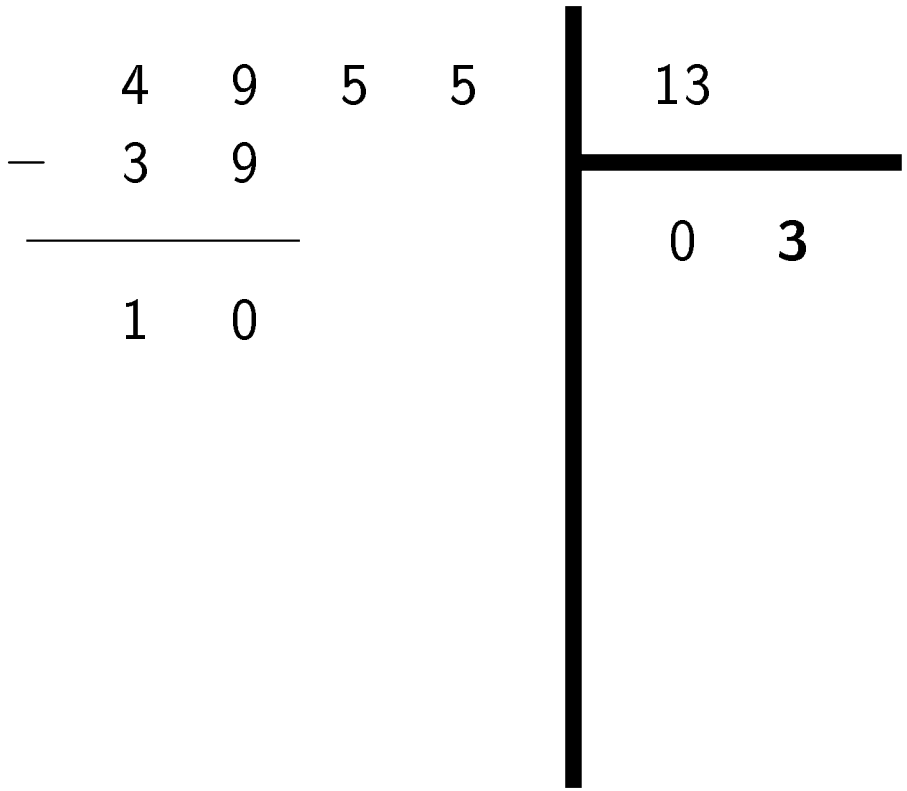
2) Algorithme du primaire

Exemple : $4955 \div 13$



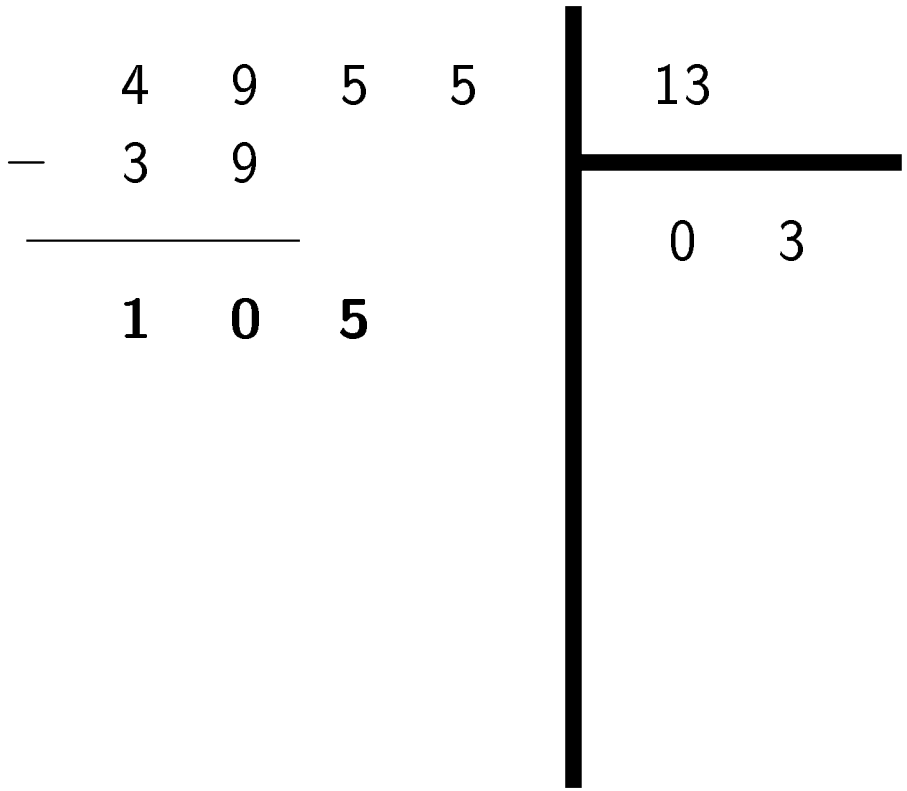
2) Algorithme du primaire

Exemple : $4955 \div 13$



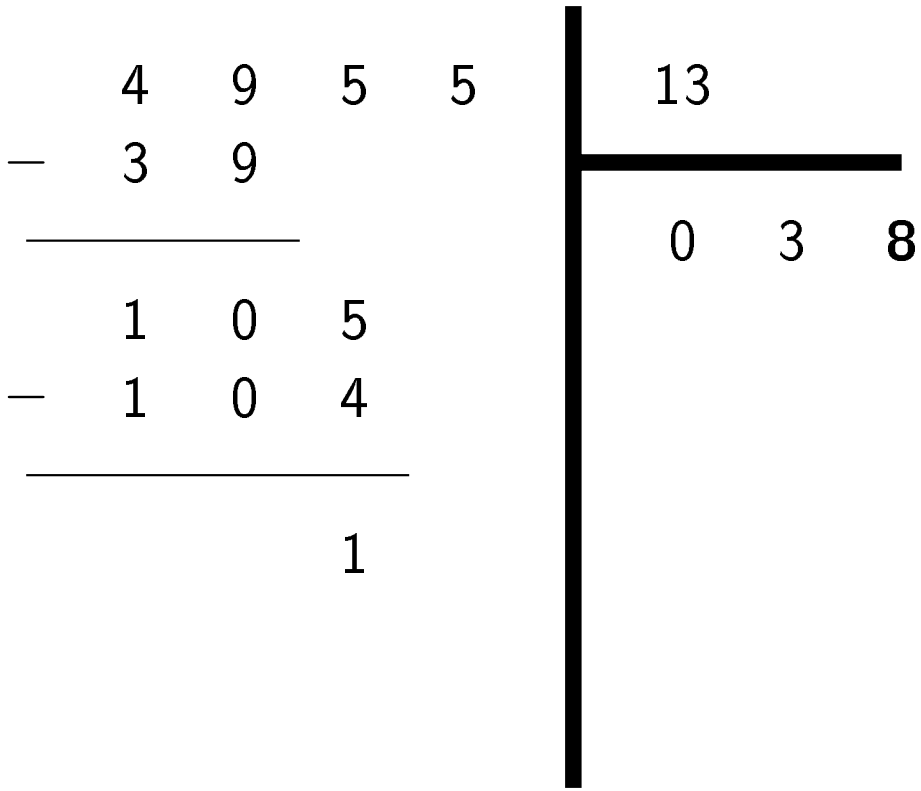
2) Algorithme du primaire

Exemple : $4955 \div 13$



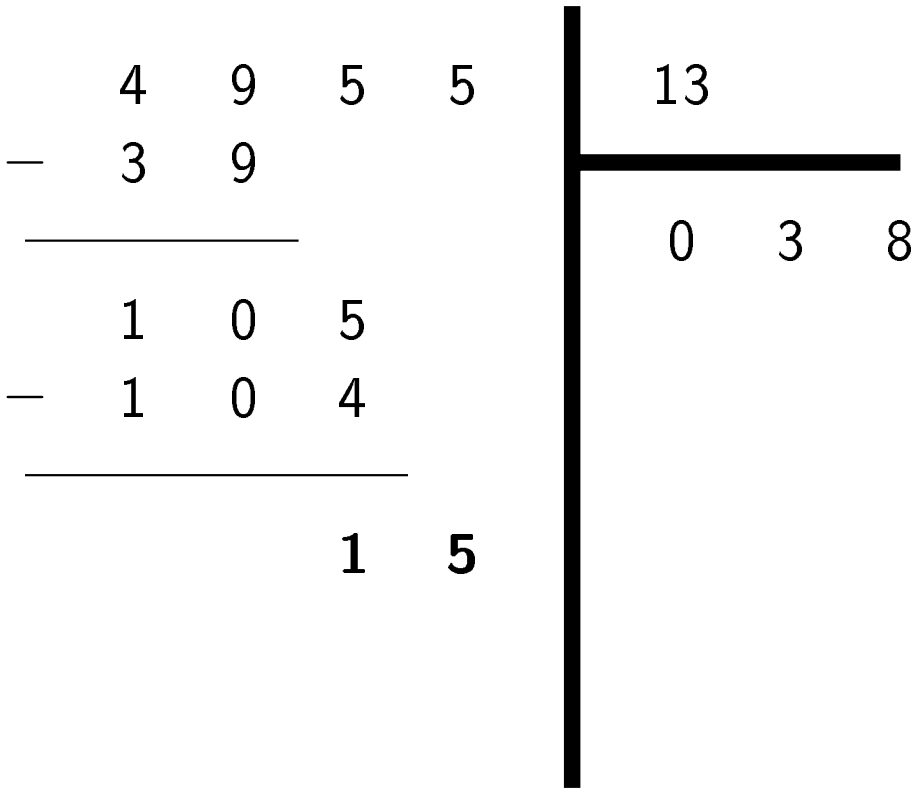
2) Algorithme du primaire

Exemple : $4955 \div 13$



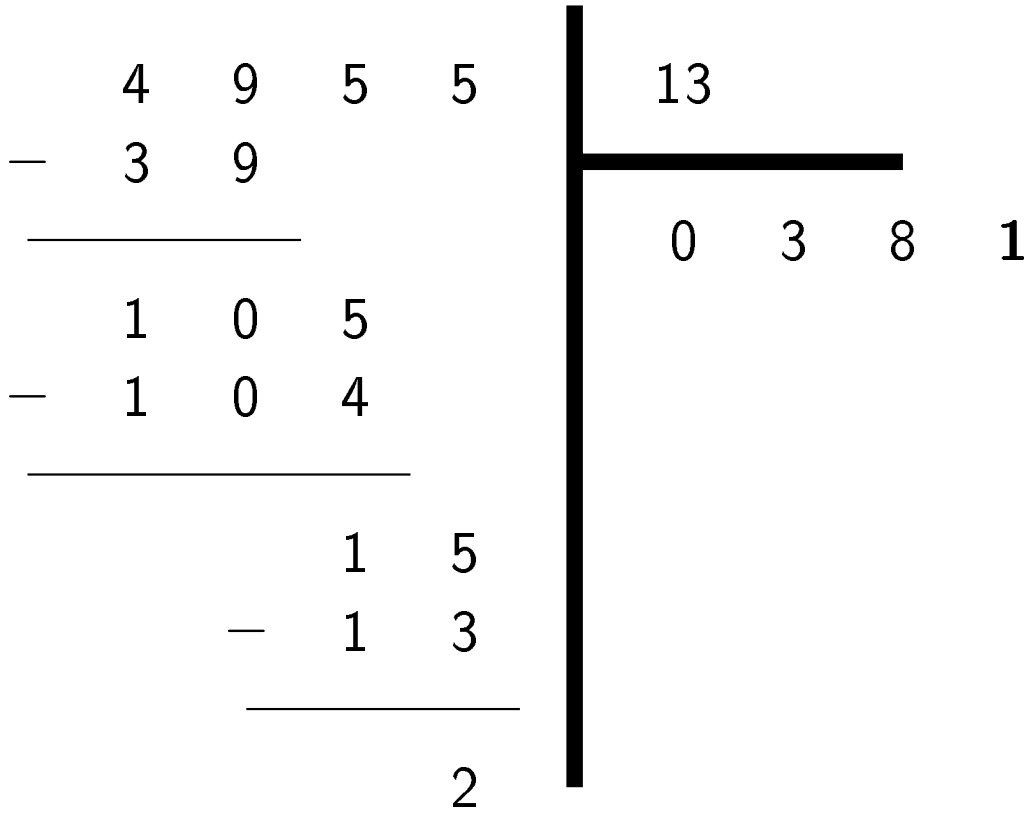
2) Algorithme du primaire

Exemple : $4955 \div 13$



2) Algorithme du primaire

Exemple : $4955 \div 13$



$$4955 = 381 \times 13 + 2$$

Exercice 2 Faites les divisions euclidiennes à la main

a) $3864 \div 7$

b) $25856 \div 21$

1. Sur TI, avec `math` ; `reste` on peut faire par exemple `reste(18,5)` qui renvoie le reste de $18 \div 5$.
2. Sur Numworks, `rem(18,5)` (« rem » pour *remainder*) fait de même.
3. Des Casio collège ont une touche $\vdash$ qui fait la division euclidienne.

II. Multiple

1) Définition

a et b entiers. On dit que a **est multiple** de b si on peut trouver $q \in \mathbb{Z}$ tel que :

$$a = q \cdot b$$

càd reste nul.

On dit aussi : b **divise** a ou encore b **diviseur** de a.

Exercice 3

a) Donner le seul entier qui est multiple de tous les autres.

b) Donner les seuls entiers qui sont diviseurs de tous les autres.

c) Donner les diviseurs positifs de 28.

2) Somme

Si m et n sont multiples de a, alors $m + n$ est multiple de a.

$m - n$ aussi

2) Somme

Si m et n sont multiples de a, alors $m + n$ est multiple de a.

$m - n$ aussi

Exemple : 18 et 24 sont multiples de 6 $\Rightarrow 18 + 24 = 42$ est multiple de 6.

2) Somme

Si m et n sont multiples de a, alors $m + n$ est multiple de a.

$m - n$ aussi

Exemple : 18 et 24 sont multiples de 6 $\Rightarrow 18 + 24 = 42$ est multiple de 6.

Attention : Réciproque fausse.
18 est multiple de 6,
$11 + 7 = 18$
mais 11 et 7 ne sont pas multiples de 6.

Exercice 4 Démonstration de la propriété

a) Traduire l'hypothèse m multiple de a.

b) Traduire l'hypothèse n multiple de a.

c) En déduire $m+n$ multiple de a. *Même chose pour* $m-n$

Exercice 5 Un nombre de 3 chiffres s'écrit $\overline{CDU}$ où C est le chiffre des centaines, D le chiffre des dizaines et U le chiffre des unités.

La barre horizontale sert à dire que les 3 chiffres forment un nombre.
On sait que $\overline{CDU} = C \times 100 + D \times 10 + U$.

a) Justifiez que $U = 0$ ou $U = 5 \Rightarrow \overline{CDU}$ multiple de 5.

b) Montrez la réciproque.

Exercice 6 $\overline{CDU} = C \times 99 + D \times 9 + (C + D + U)$

a) Justifiez que $C + D + U$ multiple de $3 \Rightarrow \overline{CDU}$ multiple de 3.

b) Montrez la réciproque.

3) pair, impair

Un entier a est **pair ssi** il est multiple de $2 \Leftrightarrow a = 2\,n$ pour un certain entier n.

3) pair, impair

Un entier a est **pair ssi** il est multiple de $2 \Leftrightarrow a = 2\,n$ pour un certain entier n.

Un entier a est **impair ssi** il n'est pas pair $\Leftrightarrow$ il s'écrit $a = 2\,n + 1$ pour un certain entier n.

Exercice 7 Démonstration que a impair $\Leftrightarrow a = 2n + 1$.

a) **Sens** $\Rightarrow$ on suppose a impair.

La division euclidienne de a par 2 donne $a = 2q + r$.
Quelles sont les valeurs possibles de r ?
Pourquoi $r = 0$ est impossible ? Conclure.

b) **Sens** $\Leftarrow$ on suppose $a = 2n + 1$.
Raisonnons par l'absurde en supposant a pair.

Montrer qu'alors 1 est multiple de 2. Conclure.

Exercice 8 Sur le modèle de l'exercice 5, montrez que :

a pair **ssi** le chiffre des unités de a est pair.

Exercice 9 Montrer que :

a) Le carré d'un nombre pair est pair.

b) Le carré d'un nombre impair est impair.

Exercice 10 n est impair.

Montrer que $n^2 = 4k + 1$ pour un certain k entier.

4) Fraction irréductible

Soit $x \in \mathbb{Q} \Leftrightarrow$ On peut écrire $x = \dfrac{p}{q}$ où $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$.

Si p et q ont un diviseur commun, hormis 1 ou -1, on peut simplifier la fraction.

$$\frac{42}{30} = \frac{21 \times \cancel{2}}{15 \times \cancel{2}} = \frac{7 \times \cancel{3}}{5 \times \cancel{3}} = \frac{7}{5}$$

La fraction est **irréductible** quand **numérateur** et **dénominateur** n'ont plus de diviseur commun.

On peut toujours mettre une fraction sous forme irréductible.

Exercice 11 Mettre les fractions sous forme irréductible.

a) $\frac{178}{55}$ b) $\frac{45}{10}$ c) $\frac{936}{441}$ d) $\frac{-144}{180}$

Exercice 12 On veut démontrer que $\sqrt{2} \notin \mathbb{Q}$.

Par l'absurde : on va supposer que $\sqrt{2} \in \mathbb{Q}$, c'est à dire qu'il est possible d'écrire $\sqrt{2} = \frac{p}{q}$.

On peut toujours choisir une forme $\frac{p}{q}$ irréductible.

On a donc $2 = \frac{p^2}{q^2}$

a) Justifier que p^2 est pair. En déduire la parité de p.

b) Puisque $p = 2\,p'$, justifier que q^2 est pair.
En déduire la parité de q.

c) Conclure.

Exercice 12 Montrez que $\frac{2n+3}{2n+1}$ est toujours une fraction irréductible.

III. Nombre premier

Dans cette section, on se limite à $\mathbb{N}$.

1) Définition

$p \in \mathbb{N}$ est premier **ssi** p a exactement 2 diviseurs $\in \mathbb{N}$ **distincts**, 1 et lui même.

1 n'est pas premier.

Exercice 13 Crible d'Eratosthène.

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

i) Prendre la première case non rayée et non entourée.
ii) Entourer la case, relever sa valeur a.
iii) Faire des sauts de a cases et rayer toutes les cases rencontrées.
iv) Recommencer jusqu'à rayer ou entourer toutes les cases.

Exercice 14 On prouve que l'ensemble des nombres premiers est infini.
Par l'absurde : Supposons que p est le plus grand des nombres premiers.

a) Justifiez que $Q = 1 \times 2 \times \cdots \times p + 1$ est plus grand que p.

b) Justifiez que Q n'est divisible par aucun entier $\leq p$ hormis 1.

c) Conclure.

Exercice 15 On considère un premier $p \geq 6$.

$p = 6 \cdot q + r$, avec $q \geq 1$ et $0 \leq r < 6$.

a) Justifier que r ne peut être 0, 2, 3 ou 4.

b) Les entiers de forme $6\,k + 1$ et $6\,k + 5$ avec $k \geq 1$ sont-ils tous des premiers ?

Exercice 16 Deux nombres premiers sont dit jumeaux lorsque leur différence est de 2.

1) Proposer quelques exemples de nombres premiers jumeaux.
2) Soit $p \geq 6$ le plus grand des deux jumeaux. On sait (exo précédent) que l'on peut écrire $p = 6k + 1$ ou $p = 6k + 5$.
   a) Puisque $p - 2$ est premier aussi, justifier que $p = 6k + 1$.
   b) Les paires $(6k + 1\,; 6k - 1)$ sont elles tous des premiers jumeaux ?

Exercice 17 Soit p un premier $p \geq 6$.

Montrer que $p^2 = 24k + 1$ pour un k entier.

2) Théorème fondamental

Tout nombre de $\mathbb{N}$ admet une **décomposition unique** en produit de facteurs premiers.

Exemple :

$$24\,255 = 3 \times 3 \times 5 \times 7 \times 7 \times 11$$

Exercice 18 Faites la décomposition en facteurs premiers des nombres suivants.

a) 426
b) 355
c) 80
d) 510

Exercice 19 On veut prouver que $\frac{1}{3} \notin \mathbb{D}$.

Par l'absurde, supposons $\frac{1}{3} \in \mathbb{D}$. Alors on peut écrire :

$$\frac{1}{3} = \frac{a}{10^n} \Leftrightarrow 10^n = 3 \cdot a$$

Pour un certain entier a et un certain entier n.

a) Faites la décomposition en facteurs premiers de 10^n.
b) Conclure.

IV. PGCD

On se limite à $\mathbb{N}$.

$a, b \in \mathbb{N}$ avec $(a, b) \neq (0, 0)$.

Le PGCD de a et b est le plus grand diviseur commun à a et b.

$$PGCD(35, 15) = \cdots \quad ; \quad PGCD(45, 15) = \cdots \quad ; \quad PGCD(34, 39) = \cdots$$

On se limite à $\mathbb{N}$.

$a, b \in \mathbb{N}$ avec $(a, b) \neq (0, 0)$.

Le PGCD de a et b est le plus grand diviseur commun à a et b.

$$PGCD(35, 15) = \cdots \quad ; \quad PGCD(45, 15) = \cdots \quad ; \quad PGCD(34, 39) = \cdots$$

Deux nombres a et b tels que $PGCD(a, b) = 1$

Exercice 20 Existence du PGCD

1) Cas $a = b = 0$.
   a) Quel est l'ensemble des diviseurs de a et b ?
   b) Le PGCD existe-t-il ?
2) Cas $a \neq 0$. Soit q diviseur de a, alors $a = q \cdot q'$
   a) Justifier que $q \geq 1$.
   b) En déduire que $q' \leq a$.
   c) Justifier que a et b ont toujours au moins un diviseur en commun.
   d) En conclure l'existence du PGCD de a et b.

Exercice 21 Algorithme d'Euclide

Soient a et b deux entiers, $(a, b) \neq (0, 0)$.

1) Si $b = 0$, justifier que $PGCD(a, b) = a$.
2) Si $b \neq 0$, alors $a = b \cdot q + r$.
   a) Montrer que tout diviseur commun de a et b divise aussi r.
   b) Montrer que tout diviseur commun de b et r divise aussi a.
   c) Conclure que $PGCD(a, b) = PGCD(b, r)$.

On en déduit l'algorithme d'Euclide :

```
def PGCD(a,b):
    assert not a,b == 0, 0
    if b == 0:
        return a
    else:
        return PGCD(b, a%b)
```

Exercice 22 Calculer le PGCD de a et b.

a) $a = 159\,058$ et $b = 5\,382$

b) $a = 2\,325$ et $b = 1\,155$