Arithmétique : Diviseurs, division euclidienne et congruences.

L'arithmétique est l'étude des nombres entiers.
Il faudra veiller à respecter le cadre d'étude dans lequel on se trouve : $\mathbb{N}$ ou $\mathbb{Z}$.
Il est bien pratique de pouvoir travailler avec des entiers positifs, mais cela n'est pas toujours possible. Il faut donc savoir faire les deux.

1) Diviseurs et multiples :

Définition 1 : Soit a un entier relatif non nul et b un entier relatif : $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$.

a* divise *b si et seulement si : il existe un entier relatif k tel que $b = k \times a$.

Autre formulations possibles : ***b* est multiple de *a***.

Ou encore : a est un diviseur de b ; b est divisible par a.

Exemples : Pour trouver des diviseurs, on écrit des multiplications.

- $12 = 3 \times 4$ donc 3 et 4 divisent 12 ;
- 5 ne divise pas 8 car $8 = 1,6 \times 5$ et $1,6 \notin \mathbb{Z}$;
- -3 divise 21 car $21 = 7 \times (-3)$ et $7 \in \mathbb{Z}$;
- 5 divise -15 car $-15 = (-3) \times 5$ et $-3 \in \mathbb{Z}$.

Quelques remarques évidentes :

- 0 n'est **jamais** un diviseur, car un diviseur ne peut jamais être nul ;
- mais 0 est multiple de tous les nombres entiers et tout entier non nul divise 0 ;
- tout entier $n \neq +/-1$ possède quatre diviseurs : 1 et -1, puis n et $-n$.

Notations :

- ***a* divise *b*** s'écrit mathématiquement : $a|b$;
- les multiples de 3 sont les nombres de l'ensemble $3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$;
- **l'ensemble des multiples de *n*** se note $n\mathbb{Z} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}$.

Deux conséquences de la définition :

- si a divise b et $b \neq 0$, alors $|a| \leqslant |b|$ (a est plus petit que b en valeur absolu) ;
- si a divise b et b divise a, alors : soit $a = b$ soit $a = -b$.

Remarque : Diviseurs et multiples sont donc deux notions équivalentes.

Exercice :

i) Rechercher les diviseurs positifs de 42 puis de 100.
ii) Expliquer comment on peut obtenir tous les diviseurs positifs d'un entier naturel n, en balayant uniquement ceux qui sont inférieurs ou égaux à $\sqrt{n}$.

Exercice :

i) Montrer que le produit de deux entiers consécutifs est pair. Et leur somme ?
ii) Montrer que la somme de trois entiers consécutifs est multiple de trois.
iii) Déterminer les entiers **relatifs** n tels que $n-2$ divise $n+3$.
iv) Démontrer que n^2 et n ont la même parité.
v) En déduire que $\sqrt{2}$ est irrationnel.

Propriété 1 : Soit a, b et c trois entiers relatifs : $a\in\mathbb{Z}$, $b\in\mathbb{Z}$ et $c\in\mathbb{Z}$.

Si a divise b et a divise c alors :

a divise toutes **combinaisons linéaires** de b et c, c'est-à-dire toutes les expressions de la forme :

$$\alpha b+\beta c \text{ où } \alpha\in\mathbb{Z} \text{ et } \beta\in\mathbb{Z}.$$

preuve :

si a divise b alors il existe un entier relatif q tel que $b=qa$
si a divise c alors il existe un entier relatif q' tel que $c=q'a$

prenons maintenant deux entiers relatifs quelconques α et β

alors $\alpha b+\beta c=\alpha qa+\beta q'a=(\alpha q+\beta q')a$ donc a divise bien $\alpha b+\beta c$.

En particulier : Si un entier n divise deux entiers a et b, alors il divise :

- leur somme $a+b$;
- leur différence $a-b$;
- et toute expression du type $3a-5b$ par exemple.

Applications :

i) Quels sont les diviseurs communs à deux entiers consécutifs ?
ii) Déterminer les entiers **naturels** qui divisent en même temps $2k+1$ et $3k-2$, $k\in\mathbb{Z}$.

Exercice : Soient a , b et c trois entiers relatifs non nuls.

Démontrer que la divisibilité est une **propriété transitive**, c'est-à-dire que :

$$\text{Si } \begin{cases} a \text{ divise } b \\ b \text{ divise } c \end{cases} \text{ alors } a \text{ divise } c$$

2) Critères de divisibilité :

Règles 1 : Par une terminaison : 2 , 5 , 10 , 25 , 4 .

Un entier est divisible par 2 s'il se termine par 0 , 2 , 4 , 6 ou 8 .

Un entier est divisible par 5 s'il se termine par 0 ou 5 .

Un entier est divisible par 10 s'il se termine par 0 .

Un entier est divisible par 25 s'il se termine par 00 , 25 , 50 , ou 75 .

Un entier est divisible par 4 si ses deux derniers chiffres forment un nombre divisible par 4 .

Règles 2 : Par une somme de ses chiffres.

Un entier est divisible par 3 , respectivement par 9 , si et seulement si la somme de ses chiffres est divisible par 3 , respectivement par 9 .

Règles 3 : Par différence de ses chiffres : 11 .

Un entier est divisible par 11 si la somme de ses chiffres extrêmes est égale à celui du milieu.

572 est divisible par 11 *car* : $2+5=7$. On a alors $572=11\times52$.

D'une façon générale un entier est divisible par 11 si la différence entre la somme de ses chiffres de rang pairs et la somme de ses chiffres de rang impairs est elle aussi divisible par 11 .

5 874 est divisible par 11 car : $(4+8)-(7+5)=12-12=0$ et 0 est divisible par 11
1 958 est divisible par 11 car : $(8+9)-(5+1)=17-6=11$ et 11 est divisible par 11.

3) Division euclidienne :

Comme en général deux entiers ne se divisent pas, intéressons-nous au mécanisme des divisions.

Exemples : Posez les divisions euclidiennes suivantes et les traduire par une égalité.

275 par 13 275 par -13 -275 par 13 -275 par -13

Définition 2 : La division euclidienne.

Soit b un entier relatif non nul.

Tout entier a s'écrit de manière unique sous la forme :

$$\boldsymbol{a = bq + r} \text{ avec } \boldsymbol{q} \in \mathbb{Z} \text{ et } \boldsymbol{0 \leqslant r < |b|}.$$

$\boldsymbol{q}$ est appelé le **quotient** et $\boldsymbol{r}$ le **reste** de **la division euclidienne de $\boldsymbol{a}$ par $\boldsymbol{b}$** , qui est le mécanisme qui fait correspondre au couple (a, b) l'unique couple (q, r) vérifiant ces conditions.

Attention, car le reste $\boldsymbol{r = a - bq}$ **doit toujours être positif !**

Concernant la partie entière de a/b , notée $E(a/b)$:

si $b > 0$ alors $E(a/b) = q$
si $b < 0$ et a/b est entier alors $E(a/b) = q$, sinon $E(a/b) = q - 1$

preuve 1 : en utilisant la partie entière.

Pour $b > 0$: on pose $q = E(a/b)$ et $r = a - bq$.

De l'inégalité $q \leqslant a/b < q + 1$ on déduit aisément $0 \leqslant r < b$ et donc $0 \leqslant r < |b|$.

Pour $b < 0$, deux cas se présentent :

- Soit a/b est entier, dans quel cas $a = bq + 0$ en posant $q = E(a/b)$ qui est entier.
- Soit a/b n'est pas entier, et alors on pose $q = E(a/b) + 1$ et $r = a - bq$.

De l'inégalité $q - 1 \leqslant a/b < q$ on déduit aisément $0 < r \leqslant -b$.
Mais $r = -b$ est impossible, car alors $a = (q-1)b$ et a/b serait un entier.
Finalement, on a bien $a = bq + r$ et $0 \leqslant r < |b|$.

En ce qui concerne l'unicité maintenant.

Si a s'écrit $a=bq+r=bq'+r'$ alors $b(q-q')=r'-r$.
Donc b divise $r'-r$. Comme $0\leqslant r<|b|$ et $0\leqslant r'<|b|$, nécessairement $|b|>|r'-r|$.
Alors nécessairement $r'-r=0$, et donc $q'=q$.

preuve 2 :

En utilisant uniquement les propriétés de $\mathbb{N}$, en montrant que le quotient q est le plus grand entier tel que $bq\leqslant a$, ou que $q+1$ est le plus petit entier tel que $a<(q+1)b$.

- Supposons dans un premier temps $a\geqslant 0$ et $b>0$.
Soit E l'ensemble des entiers naturels k tels que $a<kb$, qui est une partie de $\mathbb{N}$.
Montrons que E est non vide.
En effet, $(a+1)b=ab+b>ab\geqslant a$ puisque $b\geqslant 1$; donc $a+1$ est élément de E.
Donc E possède un plus petit élément x.
Comme $xb>a$ et que $a\geqslant 0$ alors $x>0$ donc $x\geqslant 1$.
On peut alors poser $q=x-1\in\mathbb{N}$.
Comme $x=min(E)$, $q=x-1\notin E$, ce qui donne : $qb\leqslant a<(q+1)b$ soit $qb\leqslant a<qb+b$.
En posant $r=a-bq$ il vient $0\leqslant r<b$ ce qui prouve l'existence du couple (q,r).

- Passons maintenant au cas où $a<0$.
Posons $a'=a(1-b)$.
Comme $a<0$ et $b\geqslant 1$ alors $a'\geqslant 0$.
On peut alors appliquer le cas précédent pour obtenir un couple (q',r)
tel que $a'=bq'+r$ et $0\leqslant r<b$.
Alors $a'=a(1-b)=a-ba=bq'+r$ donc $a=ba+bq'+r=b(q'+a)+r$.
Et en posant $q=q'+a$ on obtient l'existence du couple (q,r) tel que $a=bq+r$.

- Passons maintenant au cas où $b<0$.
La division de a par $-b$ donne $a=-bq+r=b(-q)+r$ avec $0\leqslant r<-b$ ou encore $0\leqslant r<|b|$.

- Et finalement l'unicité.

Supposons l'existence de deux couples (q_1,r_1) et (q_2,r_2) tels que $a=bq_1+r_1=bq_2+r_2$.
Alors $r_1-r_2=b(q_2-q_1)$ donc r_1-r_2 est un multiple de b.
Comme $0\leqslant r_1<|b|$ et $0\leqslant r_2<|b|$, alors $-|b|<r_2\leqslant 0$ et donc $-|b|<r_1-r_2<|b|$.
Ainsi r_1-r_2 est un multiple de b strictement compris entre $-|b|$ et $|b|$.
La seule possibilité est que r_1-r_2 soit nul. Ce qui donne ensuite $q_1=q_2$.

https://ljk.imag.fr/membres/Bernard.Ycart/mel/ar/node4.html

Tous les résultats d'arithmétique reposent sur l'existence de la division euclidienne.
Il est donc primordiale de maîtriser sa manipulation.
Ainsi, le rapport entre deux entiers a et b repose sur l'égalité unique :

$$a = bq + r \text{ avec } 0 \leqslant r < |b|$$

On évitera donc d'écrire des divisions en arithmétique.

Applications :

i) Trouver tous les entiers qui divisés par 5 donne un quotient égal à trois fois le reste.
ii) Lorsqu'on divise a par b le reste est 8 et lorsqu'on divise $2a$ par b le reste est 5. Trouver le diviseur b.

Exercice : On donne $220 = 13 \times 17 - 1$.

i) En déduire le quotient et le reste de la division euclidienne de 220 par 13.
ii) n déduire le quotient et le reste de la division euclidienne de -220 par 13.
iii) Puis ceux de 220 par -13.

4) Congruences :

On s'intéresse maintenant aux nombres qui possèdent un même reste dans la division euclidienne par un entier naturel n, donc au moins égal à 2.

Définition 3 : Soit un entier $n \geqslant 2$, et deux entiers relatifs a et b.

a est **congru** à b **modulo** n si et seulement si a et b ont le même reste dans la division euclidienne par n, donc si et seulement si n divise $b-a$.

notation : a est congru à b modulo n s'écrit : $a \equiv b\,[n]$.

Exemples :

1) Un nombre est toujours congru à son propre reste dans la division par n :

$$2019 = 9\,[10] \qquad 50 = 1\,[7] \qquad 65 = 2\,[9]$$

2) Si $x = 0\,[2]$ alors x est pair et si $x = 1\,[2]$ alors x est impair.

Propriété 2 : La congruence est une **relation d'équivalence**.
Cela signifie qu'elle est réflexive, symétrique, et transitive (RST).

Réflexive car $a \equiv a[n]$
Symétrique car si $a \equiv b[n]$ alors $b \equiv a[n]$
Transitive car si $a \equiv b[n]$ et $b \equiv c[n]$, alors $a \equiv c[n]$

Exercice : Quel jour sera-t-on dans 1 an, 300 jours, 100 jours ?
Quel jour était-on il y a 1 an, 300 jours ou 100 jours ?

Propriété 3 :

$\boldsymbol{a \equiv b(n)}$ si et seulement si $\boldsymbol{a - b \equiv 0[n]}$

ou si et seulement si $\boldsymbol{a - b \in n\mathbb{Z}}$

ou si et seulement si $\boldsymbol{n}$ divise $\boldsymbol{a - b}$

ou si et seulement si il existe $\boldsymbol{k \in \mathbb{Z}}$ tel que $\boldsymbol{a = b + kn}$.

preuve : on doit démontrer la propriété dans les deux sens.

Sens $\Rightarrow$ ou CN pour condition nécessaire

On sait que $a \equiv b[n]$ donc il existe q, q' et r tels que :

$a = nq + r$ et $b = nq' + r$ avec $0 \leqslant r < n$

On en déduit que $a - b = n(q - q')$, donc $a - b$ est un multiple de n,
donc son reste dans la division par n est nul, donc $a - b \equiv 0[n]$.

Sens $\Leftarrow$ ou CS pour condition suffisante

On sait que $a - b \equiv 0[n]$ donc il existe k tel que $a - b = kn$

Si l'on effectue la division de a par n, on peut écrire $a = nq + r$

Ceci donne : $nq + r - b = kn$ et donc $b = nq - kn + r = (q - k)n + r$

Alors b a le même reste que a dans la division par n, donc $a \equiv b[n]$.

Propriété 3 : Les règles opératoires avec les congruences.

Supposons $a \equiv b[n]$ et $c \equiv d[n]$ où $n \geqslant 2$.

Alors : $a + b \equiv b + d[n]$ et $a - c \equiv b - d[n]$

$a \times c \equiv bd[n]$

$k \times a \equiv k \times b[n]$ pour tout entier relatif k .

$a^k \equiv b^k[n]$ pour tout entier naturel k .

preuve :

1) *Compatibilité avec l'addition.*
On sait que : $a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc $(a-b)$ et $(c-d)$ sont des multiples de n. Il existe donc deux entiers relatifs k et k' tels que :

$$a - b = kn \quad \text{et} \quad c - d = k'n$$

En additionnant ces deux égalités, on obtient :

$$a - b + c - d = kn + k'n$$
$$(a + c) - (b + d) = (k + k')n$$

Donc $(a + c) - (b - d)$ est un multiple de n, donc d'après le théorème 2, on obtient :

$$a + c \equiv b + d\ (n)$$

2) *Compatibilité avec la multiplication.*
On sait que : $a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc, il existe deux entiers relatifs k et k' tels que :

$$a = b + kn \quad \text{et} \quad c = d + k'n$$

En multipliant ces deux égalités, on obtient :

$$ac = (b + kn)(d + k'n)$$
$$ac = bd + k'bn + kdn + kk'n^2$$
$$ac = bd + (k'b + kd + kk'n)n$$
$$ac - bd = (k'b + kd + kk'n)n$$

Donc $(ac - bd)$ est un multiple de n, donc d'après le théorème 2, on a :

$$ac \equiv bd\ (n)$$

3) *Compatibilité avec les puissances.*
On prouve cette compatibilité par récurrence sur k, à l'aide de la compatibilité avec la multiplication. Nous en confions la preuve au lecteur.

Remarque et notation :

Dans la division par l'entier n , les restes possibles, ou résidus, sont les entiers de l'ensemble noté $\mathbb{Z}/n\mathbb{Z}=\{0,1,2,\ldots,n-1\}$.

Exercices :

Congruences et opérations arithmétiques, congruences et restes ou critères de divisibilité..

Algorithme :

On réalise un algorithme pour afficher tous les diviseurs d'un nombre entier naturel n .
Les diviseurs sont stockés dans une liste [] d'abord vide.
L'algorithme s'arrête lorsque le diviseur d dépasse $\sqrt{n}$.
Lorsque ce diviseur d convient, on l'ajoute à la liste des diviseurs.

```
1  # la liste des diviseurs d'un entier
2  from math import sqrt
3  n = int(input("donner un entier"))
4  diviseurs = []
5  d = 0
6  while d <= sqrt(n):
7      d = d + 1
8      if n % d == 0:
9          diviseurs.append(d)
10 print(diviseurs)
```

```
*** Console de processus distant Réinitialisée ***
>>>
[1, 2, 3, 4, 5, 6, 8, 10]
>>>
```

Exercices : Pour s'amuser sur les dates par exemple.

Combien y-a-t-il d'années bissextiles entre le 1er janvier 1998 et 1er janvier 2042 ?
Combien y-a-t-il de jours entre le 1er janvier 2012 et le 1er janvier 2042 ?
Pourriez-vous trouver le jour de votre naissance.

Attention, car on ne peut pas simplifier une équation de congruence :

Si $a\times c \equiv b\times c\,(n)$ alors on n'a pas nécessairement $a \equiv b\,(n)$

Nous démontrerons ultérieurement que pour pouvoir effectuer cette simplification, il est nécessaire que c soit premier avec n .

Liste des diviseurs d'un entier :

Pour dresser la liste des diviseurs d'un entier, il suffit d'écrire toutes les multiplications qui donnent cet entier, en s'arrêtant dès que possible.

Par exemple $90 = 1\times 90 = 2\times 45 = 3\times 30 = 5\times 18 = 6\times 15 = 9\times 10$

Donc l'ensemble des diviseurs de 90 est $D_{90}=\{1;2;3;5;6;9;10;15;18;30;45;90\}$

Une expression du type $15p^2-39q^3$ est divisible par trois car 15 et 39 le sont.

Une expression du type $3k+7$ n'est jamais divisible par trois, car 7 ne l'est pas.

Mais l'expression $2n^2-n+3$ est-elle divisible par 3 pour tout n ?

Exercices :

1) Donner le quotient et le reste dans la division par 23 de 10 000 et – 10 000 .

2) Donner le reste dans la division euclidienne de 2020^{2020} par 13 .

3) Montrer que 3^n+7^n est un entier divisible par 4 pour tout entier n .