Multiples. Division euclidienne. Congruence

Table des matières

1 Avant propos

L'arithmétique concerne l'étude des entiers naturels $\mathbb{N}$ ou relatifs $\mathbb{Z}$.
$\mathbb{N}$ est l'ensemble des entiers naturels : $0, 1, 2, 3, \ldots$
$\mathbb{Z}$ est l'ensemble des entiers relatifs : $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$

- La résolution d'exercices peut donc se faire soit dans $\mathbb{N}$ soit dans $\mathbb{Z}$.
- Le mode de résolution dans les ensembles $\mathbb{N}$ ou $\mathbb{Z}$ est différent de la résolution dans $\mathbb{R}$. La résolution en arithmétique demande beaucoup d'intuition et de rigueur. C'est ce qui fait la spécificité de l'arithmétique, « *la plus belle des disciplines* » selon Friedrich Gauss

Propriété 1 : Axiomes dans $\mathbb{N}$

Principe du bon ordre : toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Principe de descente infinie : toute suite dans $\mathbb{N}$ strictement décroissante est finie (se termine après un nombre fini de termes).

Principe des tiroirs : si l'on range $(n+1)$ chaussettes dans n tiroirs, alors un tiroir contiendra au moins deux chaussettes.

Exemple : Un exemple du principe des tiroir. Dans la division par 7 d'un entier non multiple de 7, les restes possibles sont 1, 2, 3, 4, 5 et 6, on est alors sûr qu'à partir de la 7^e division, donnant la 7^e décimale, on obtiendra un reste déjà obtenu.
Par exemple la partie décimale de : $\dfrac{22}{7} = 3,142857\,142857\ldots$ est périodique.

2 Divisibilité dans $\mathbb{Z}$

2.1 Définition

Définition 1 : Soit a et b deux entiers relatifs.
On dit que b divise a, noté $b|a$, si et seulement si, il existe un entier relatif k tel que :
$$a = kb, \quad k \in \mathbb{Z}$$

Remarque : Autres formulations possibles :
« b est un diviseur de a », « a est divisible par b », « a est un multiple de b ».

Exemples :

- $54 = 6 \times 9$ donc 6 et 9 sont des diviseurs de 54.
  Les diviseurs de 54 dans $\mathbb{N}$ sont : 1, 2, 3, 6, 9, 18, 27, 54
- $-45 = (-9) \times 5$ donc -9 et 5 sont des diviseurs de -45.
  Les diviseurs de -45 dans $\mathbb{Z}$ sont : $-45, -15, -9, -5, -3, -1, 1, 3, 5, 9, 15, 45$

2.2 Propriétés

- 0 est multiple de tout entier a car : $0 = 0 \times a$. Multiple universel.
- 1 divise tout entier a car : $a = 1 \times a$. Diviseur universel.
- Si a est un multiple de b et si $a \neq 0$ alors : $|a| \geqslant |b|$.
- Si a divise b et si b divise a alors $a = b$ ou $a = -b$ avec a et b non nuls.

2.3 Règles de divisibilité

Toutes les règles de divisibilité peuvent être démontrées par la congruence (partie 4 de ce chapitre).

Règle 1 : Par une terminaison : 2, 5, 10, 25, 4

- Un entier est divisible par 2 s'il se termine par 0, 2, 4, 6, 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, 75.
- Un entier est divisible par 4 si le nombre formé par ses 2 derniers chiffres est divisible par 4.
  1 9**32** est divisible par 4 mais pas 1 7**14**.

Règle 2 : Par somme de ses chiffres : 3 et 9

- Un entier est divisible par 3 (respectivement par 9) si la somme de ses chiffres est divisible par 3 (respectivement par 9).
  8 232 est divisible par 3 car : $8+2+3+5=15$
  4 365 est divisible par 9 car : $4+3+6+5=18$

Règle 3 : Par différence de ses chiffres : 11

- Si pour un entier de trois chiffres, la somme des chiffres extrêmes est égale à celui du milieu alors cet entier est divisible par 11.
  451 est divisible par 11 car : $4+1=5$. On a alors $\mathbf{451} = 11 \times 41$
- D'une façon générale un entier est divisible par 11 si la différence entre la somme des chiffres de rangs pairs et la somme des chiffres de rangs impairs est divisible par 11.
  6 457 est divisible par 11 car : $(7+4)-(5+6)=11-11=0$
  4 939 est divisible par 11 car : $(9+9)-(3+4)=18-7=11$

Exemple : Trouver tous les diviseurs des nombres suivants : 20, 36 et 120

On montre facilement que :

- Les diviseurs de 20 sont : 1, 2, 4, 5, 10, 20
- Les diviseurs de 36 sont : 1, 2, 3, 4, 6, 9, 12, 18, 36
- Les diviseurs de 120 sont : 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120

Algorithme : Déterminer l'ensemble de diviseur d'un entier naturel n donné.

Si d divise n, alors $n = kd$ donc le quotient k est aussi un diviseur de n.
Lorsque l'on trouve un diviseur de n, on en trouve donc un second.
Par exemple avec 120 : La première colonne s'arrête lorsque le diviseur $d > \sqrt{n}$.
On peut en Python écrire la fonction div(n) suivante.

diviseur d	quotient k
1	120
2	60
3	40
4	30
5	24
6	20
8	15
10	12

```
def div(n):
    D=[]
    i=1
    while i<=sqrt(n):
        if n%i==0:
            D.append(i)
            if n//i!=i:
                D.append(n//i)
        i+=1
    D.sort()
    return D, len(D)
```

Pour div(120) on trouve : ([1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120], 16)

2.4 Exercices d'applications

1) Déterminer tous les couples d'entiers naturels tels que : $x^2 - 2xy = 15$

2) Déterminer tous les entiers relatifs n tels que $(n-3)$ divise $n+5$

1) On cherche à mettre le terme de droite en facteur de façon à faire apparaître des diviseurs de 15. En factorisant, on trouve : $x(x-2y) = 15$

   Comme x et y sont des entiers naturels, on a la relation suivante : $x \geqslant x - 2y$.
   De plus les diviseurs de 15 sont : $D_{15} = \{1, 3, 5, 15\}$

   Les décompositions possibles sont : 15×1 ou 5×3

$$\begin{cases} x = 15 \\ x - 2y = 1 \end{cases} \quad \text{ou} \quad \begin{cases} x = 5 \\ x - 2y = 3 \end{cases}$$

$$\begin{cases} x = 15 \\ y = \dfrac{15-1}{2} = 7 \end{cases} \quad \text{ou} \quad \begin{cases} x = 5 \\ y = \dfrac{5-3}{2} = 1 \end{cases}$$

   On obtient alors les couples solutions : $(15, 7)$ et $(5, 1)$

2) Si $(n-3)$ divise $(n+5)$ alors il existe $k \in \mathbb{Z}$ tel que : $n + 5 = k(n-3)$

   On cherche à factoriser par $(n-3)$ en faisant ressortir ce terme à gauche :

$$(n-3) + 8 = k(n-3) \Leftrightarrow k(n-3) - (n-3) = 8 \Leftrightarrow (n-3)(k-1) = 8$$

donc $(n-3)$ est un diviseur de 8. L'ensemble des diviseurs de 8 dans $\mathbb{Z}$ est :

$$D_8 = \{-8, -4, -2, -1, 1, 2, 4, 8\}$$

On a donc le tableau suivant correspondant aux valeurs possibles de n :

$n-3$	-8	-4	-2	-1	1	2	4	8
n	-5	-1	1	2	4	5	7	11

2.5 Opération sur les multiples

Théorème 1 : Soit trois entiers relatifs a, b et c.
Si a divise b et c alors a divise toute combinaison linéaire de b et de c soit $\alpha b + \beta c$.

Démonstration :
On sait que a divise b et c, donc il existe deux entiers relatifs k et k' tels que :

$$b = ka \quad \text{et} \quad c = k'a$$

On a alors : $\alpha b + \beta c = (\alpha k + \beta k')a$ donc a divise $\alpha b + \beta c$

Exemple : $k \in \mathbb{N}$, on pose $a = 9k+2$ et $b = 12k+1$. Quels peuvent être les diviseurs positifs communs à a et b ?

Soit d un diviseur commun à a et b.
d divise a et b donc d divise toute combinaison linéaire de a et de b donc d divise :

$$4a - 3b = 4(9k+2) - 3(12k+1) = 36k + 8 - 36k - 3 = 5$$

$D_5 = \{1, 5\}$ d'où $d = 1$ et $d = 5$

Les diviseurs positifs possibles communs à a et b sont : 1 et 5.

3 La division euclidienne

Définition 2 : Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.
On appelle division euclidienne de a par b, l'opération qui au couple (a, b) associe l'unique couple (q, r) tel que :

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

a s'appelle le « dividende », b le « diviseur », q le « quotient » et r le « reste ».

Démonstration :

1) Montrons l'existence du couple (q, r) pour $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

- Pour $a \geqslant 0$.
  Soit E l'ensemble des entiers e tels que $be > a$.
  E n'est pas vide : en effet :
  $b \geqslant 1 \overset{\times(a+1)}{\Rightarrow} b(a+1) \geqslant a+1 \Rightarrow b(a+1) > a \Rightarrow (a+1) \in \text{E}$.

E est une partie non vide de $\mathbb{N}$ donc E admet un plus petit élément m tel que $bm > a$ et $b(m-1) \leqslant a$.

On pose alors $q = m-1$, on a alors : $bq \leqslant a < b(q+1) \overset{-bq}{\Rightarrow} 0 \leqslant a - bq < b$.
En posant $r = a - bq$ on a alors : $a = bq + r$ avec $0 \leqslant r < b$.
Il existe donc un couple (q, r) tel que : $a = bq + r$ avec $0 \leqslant r < b$.

- Pour $a < 0$.

  On pose $a' = a(1-b)$, comme $b \geqslant 1 \overset{\times(-1)}{\Rightarrow} -b \leqslant -1 \overset{+1}{\Rightarrow} 1 - b \leqslant 0$
  Donc $a' = a(1-b) \geqslant 0$, on peut alors utiliser le cas où $a \geqslant 0$ avec a' et b.
  Il existe un couple (q', r) tel que : $a' = bq' + r$ avec $0 \leqslant r < b$.
  En revenant à a, on a alors :
  $a(1-b) = bq' + r \Rightarrow a - ab = bq' + r \Rightarrow a = b(q' + a) + r$.
  En posant $q = q' + a$, on obtient alors : $a = bq + r$ avec $0 \leqslant r < b$.

2) Montrons l'unicité du couple (q, r).
On suppose qu'il existe deux couples (q, r) et (q', r') tels que :
$a = bq + r = bq' + r'$ avec $0 \leqslant r < b$ et $0 \leqslant r' < b$.
$bq + r = bq' + r' \Leftrightarrow b(q - q') = r' - r$ avec $-b < r' - r < b$.
b divise $(r' - r)$ compris strictement entre $-b$ et b donc $r' - r = 0$ d'où $r' = r$
Cela entraîne alors $q' = q$. Le couple (q, r) est unique.

Exemples :

- La division euclidienne de 114 par 8 : $114 = 8 \times 14 + 2$

114	8
2	14

- La division de -114 par 8 : $-114 = 8 \times (-15) + 6$
  En effet : $-114 = -8 \times 14 - 2 = 8 \times (-14) - 8 + 6 = 8 \times (-15) + 6$

Application :

1) Trouver les entiers qui divisés par 5 donne un quotient égal à 3 fois le reste.
2) Dans la division a par b, le reste est 8 et dans la division de $2a$ par b, le reste est 5. Déterminer le diviseur b.

1) Soit a l'entier cherché. On divise a par 5, on a alors :

$$\begin{cases} a = 5q + r \\ 0 \leqslant r < 5 \end{cases} \overset{q=3r}{\Leftrightarrow} \begin{cases} a = 15r + r = 16r \\ 0 \leqslant r < 5 \end{cases}$$

On trouve toutes les valeurs de a en faisant varier r de 0 à 4 compris, on a alors l'ensemble solution suivant : $S = \{0, 16, 32, 48, 64\}$.

2) Écrivons les deux divisions, en notant q et q' les quotients respectifs :

$$\begin{cases} a = bq + 8 \ , \ b > 8 \\ 2a = bq' + 5 \ , \ b > 5 \end{cases} \Leftrightarrow \begin{cases} 2a = 2bq + 16 \ , \ b > 8 \\ 2a = bq' + 5 \ , \ b > 5 \end{cases}$$

donc $2bq + 16 = bq' + 5 \Leftrightarrow b(2q - q') = -11 \Leftrightarrow b(q' - 2q) = 11 \ , \ b > 8$

b est donc un diviseur positif non nul de 11, supérieur à 8, donc : $b = 11$

Algorithme : Division euclidienne par soustraction successives.
Soit la fonction diviser(a,b) en Python .

- Si $a \geqslant 0$, on soustrait b tant que a est supérieur au diviseur b en incrémentant q à chaque boucle.
- Si $a < 0$, on ajoute b tant que a est négatif en décrémentant q à chaque boucle.

```
def diviser(a,b):
    q=0
    if a>=0:
        while a>=b:
            a=a-b
            q+=1
    else:
        while a<0:
            a=a+b
            q-=1
    return q,a
```

4 Congruence

4.1 Entiers congrus modulo n

Définition 3 : Soit $n \geqslant 2$ et $a, b \in \mathbb{Z}$.
On dit que les entiers a et b sont congrus modulo n si, et seulement si, a et b ont même reste dans la division euclidienne par n. On note alors :

$$a \equiv b \mod n \quad \text{ou} \quad a \equiv b\,(n) \quad \text{ou} \quad a \equiv b\,[n]$$

Exemples :
$57 \equiv 15\,(7)$ car : $57 = 7 \times 8 + 1$ et $15 = 7 \times 2 + 1$
$41 \equiv -4\,(9)$ car $41 = 9 \times 4 + 5$ et $-4 = 9 \times (-1) + 5$.

Remarque :

- Un nombre est congru à son reste modulo n dans la division euclidienne par n.
$$2019 \equiv 9\,(10) \quad 17 \equiv 1\,(4) \quad 75 \equiv 3\,(9) \quad \ldots$$
- Parité : $x \equiv 0\,(2) \Leftrightarrow x$ pair et $x \equiv 1\,(2) \Leftrightarrow x$ impair
- a est un multiple de n si et seulement si $a \equiv 0\,(n)$.

Propriété 2 : La congruence est une relation d'équivalence, pour tout a, b, c :

- Réflexive : $a \equiv a\,(n)$
- Symétrique : si $a \equiv b\,(n)$ alors $b \equiv a\,(n)$
- Transitive : si $a \equiv b\,(n)$ et $b \equiv c\,(n)$ alors $a \equiv c\,(n)$

Remarque : La notion de congruence prend tout son intérêt, dès lors qu'on s'intéresse seulement au reste, pour une propriété donnée. Pour déterminer le jour de la semaine d'une date donnée, on travaille modulo 7.

Théorème 2 : Soit $n \geqslant 2$ et $a, b \in \mathbb{Z}$: $a \equiv b\,(n) \Leftrightarrow a - b \equiv 0\,(n)$

Démonstration : Par double implication

- $a \equiv b\ (n)$. Il existe donc q, q', et r tels que :
$$a = nq + r \quad \text{et} \quad b = nq' + r \quad \text{avec} \quad 0 \leqslant r < n$$
Par soustraction terme à terme : $a - b = n(q - q')$
Donc $a - b$ est un multiple de n et donc : $a - b \equiv 0\ (n)$
- Réciproquement : $a - b \equiv 0\ (n)$. Il existe k tel que : $a - b = kn$ (1)
Si l'on effectue la division de a par n, on a : $a = nq + r$ (2)
(2) dans (1) : $nq + r - b = kn \Leftrightarrow -b = kn - nq - r \Leftrightarrow b = (q - k)n + r$
a et b ont donc même reste dans la division par n d'où $a \equiv b\ (n)$

Remarque : On pourrait donner comme définition :
« a et b sont congrus modulo n si, et seulement si, $(a - b)$ est un multiple de n. »

4.2 Compatibilité avec la congruence

Théorème 3 : Soit $n \geqslant 2$ et $a, b, c, d \in \mathbb{Z}$ vérifiant : $a \equiv b\ (n)$ et $c \equiv d\ (n)$.
La congruence est compatible :
- avec l'addition : $a + c \equiv b + d\ (n)$
- avec la multiplication : $ac \equiv bd\ (n)$
- avec les puissances : $\forall k \in \mathbb{N},\ a^k \equiv b^k\ (n)$

Démonstration :
- Compatibilité avec l'addition.
$a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc $(a - b)$ et $(c - d)$ multiples de n.
Il existe donc $k, k' \in \mathbb{Z}$ tels que : $a - b = kn$ et $c - d = k'n$.
En additionnant ces deux égalités terme à terme on obtient :
$$a - b + c - d = kn + k'n \Leftrightarrow (a + c) - (b + d) = (k + k')n$$
$(a + c) - (b - d)$ multiple de n, donc : $a + c \equiv b + d\ (n)$
- Compatibilité avec la multiplication.
$a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc, il existe $k, k' \in \mathbb{Z}$ tels que :
$$a = b + kn \quad \text{et} \quad c = d + k'n$$
En multipliant ces deux égalités terme à terme, on obtient :
$$ac = (b + kn)(d + k'n) \Leftrightarrow ac = bd + k'bn + kdn + kk'n^2$$
$$ac = bd + (k'b + kd + kk'n)n \Leftrightarrow ac - bd = (k'b + kd + kk'n)n$$
$(ac - bd)$ multiple de n, donc : $ac \equiv bd\ (n)$.
- 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.

Exemples : : Modulo 7
- $50 \equiv 49 + 1 \equiv 0 + 1 \equiv 1\ (7)$ et $100 \equiv 2 \times 50 \equiv 2 \times 1\ (7)$
- $50^{100} \equiv 1^{100} \equiv 1\ (7)$ et $100^{100} \equiv 2^{100} \equiv (2^3)^{33} \times 2 \equiv 8^{33} \times 2 \equiv 1^{33} \times 2 \equiv 2\ (7)$

4.3 Applications de la congruence

4.3.1 Divisibilité

Montrer, pour tout $n \in \mathbb{N}$, que $3^{n+3} - 4^{4n+2}$ est divisible par 11.

On utilise la compatibilité modulo 11

- $\forall n \in \mathbb{N}, \quad 3^{n+3} \equiv 3^n \times 3^3 \equiv 3^n \times 27 \overset{27\equiv 5}{\equiv} 3^n \times 5 \ (11)$ car $27 = 11 \times 2 + 5$
- $\forall n \in \mathbb{N}, \quad 4^{4n+2} \equiv (4^4)^n \times 4^2 \equiv (16^2)^n \times 16 \overset{16\equiv 5}{\equiv} (5^2)^n \times 5 \overset{25\equiv 3}{\equiv} 3^n \times 5 \ (11)$
  car $16 = 11 \times 1 + 5$ et $5^2 = 25 = 11 \times 2 + 3$
- $\forall n \in \mathbb{N}, \quad 3^{n+3} - 4^{4n+2} \equiv 3^n \times 5 - 3^n \times 5 \equiv 0 \ (11)$.
  Pour tout $n \in \mathbb{N}$, $3^{n+3} - 4^{4n+2}$ est donc divisible par 11.

4.3.2 Tableau de congruence

Déterminer les restes possibles de n^2 dans la division par 7 suivant les valeurs de l'entier relatif n. En déduire les solutions de $n^2 \equiv 2 \ (7)$.

On utilise une méthode exhaustive. On détermine, suivant les restes de n dans la division par 7, tous les restes possible de n^2. On consigne alors les résultats dans un tableau de congruence.
On note dans le tableau $n \equiv ... \ (7)$ les restes de l'entier n dans la division par 7.

$n \equiv ... \ (7)$	0	1	2	3	4	5	6
$n^2 \equiv ... \ (7)$	0	1	4	2	2	4	1

Par exemple $n \equiv 5 \ (7) \ \Rightarrow \ n^2 \equiv 25 \equiv 4 \ (7)$ car $25 = 7 \times 3 + 4$

Les restes possibles de n^2 dans la division par 7 sont : 0, 1, 2, 4.

D'après le tableau, les solutions de $n^2 \equiv 2 \ (7)$ sont $n \equiv 3 \ (7)$ ou $n \equiv 4 \ (7)$.