BAC S - THÈME 9

Arithmétique

9.1 Divisibilité - Division euclidienne

À QUOI ÇA SERT ?

Si l'on doit partager 26 objets entre 3 personnes, ça ne va pas tomber juste : on dit alors que 26 n'est pas divisible par 3. Il restera donc quelques objets, mais combien exactement ? Pour le savoir, on effectue la *division euclidienne* de 26 par 3. Pour cela on cherche le plus grand multiple de 3 inférieur à 26, à savoir 24. Chacune des 3 personnes recevra donc 8 objets et il en restera 2. On écrit $26 = 3 \times 8 + 2$.
Les mathématiciens ont vite réalisé que cette division euclidienne avait de nombreuses applications : recherche du pgcd de 2 nombres, problèmes de calendriers, cryptographie, etc.

RAPPEL DE COURS

Division euclidienne et divisibilité

Soient a un entier relatif et b un entier naturel **non nul**. Il existe un unique couple d'entiers $(q\,,r)$ tel que :

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

Vocabulaire : le nombre a s'appelle le *dividende*, le nombre b le *pseudo-diviseur* (il n'est diviseur parfait que lorsque $r = 0$...), le nombre q le *quotient* et le nombre r le *reste*.
Exemple : la division euclidienne de 46 par 7 donne pour quotient $q = 6$ et reste $r = 4$ car $46 = 7 \times 6 + 4$.
⚠ Attention, si on change le réel a en son opposé, le quotient et le reste ne vont pas se changer en leur opposé ! Par exemple, la division euclidienne de $a = -46$ par $b = 7$ ne peut pas être $-46 = 7 \times (-6) + (-4)$ car le reste d'une division euclidienne est nécessairement positif. Il faut donc écrire $-46 = 7 \times (-7) + 3$.
En langage Python, le quotient q de a par b est obtenu en écrivant $a//b$ et le reste r en écrivant $a\%b$.
Cas particulier : lorsque le reste r d'une division euclidienne est nul, on dit alors que le nombre b *divise* le nombre a. On dit aussi que le nombre a est un *multiple* du nombre b.
Propriétés de la divisibilité : (a, b et d désignent des entiers)

- Si d divise a alors d divise tout multiple de a.
- Si d divise a et b alors d divise la somme $a + b$ ainsi que la différence $a - b$.
- En généralisant les deux propriétés précédentes, on peut dire que si d divise a et b alors d divise toute *combinaison linéaire* de a et b, cela signifie que d divise $au + bv$ où u et v sont des entiers relatifs.
- Transitivité : Si d divise b et si b divise a alors d divise a.
- Si a divise b et si b divise a alors $a = b$. (Anti-symétrie)

On peut étendre le concept division euclidienne à $\mathbb{Z}$, dans ce sens qu'on autorise désormais que b soit un entier relatif non nul. Dans ce cas, il faut nuancer la condition sur le reste en écrivant qu'il existe un unique couple d'entiers (q, r) tel que :

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

Par exemple, la division euclidenne de $a = 25$ par $b = -7$ donne $25 = (-7) \times (-3) + 4$ et on a bien $0 \leqslant r < |b|$.

Q 66 - Propriétés de la divisibilité

[⋆] [19%]

Dans cet exercice, les nombres a et b désignent des entiers relatifs.

1. Développer et simplifier l'expression suivante :

$$6(2a+3b)-7(a+2b)$$

2. En déduire que si le nombre 7 divise $2a+3b$ alors il divise $5a+4b$.

3. On voudrait maintenant étudier la réciproque de la question précédente.
Pour cela, déterminer deux entiers relatifs α et β tels que :

$$6(5a+4b)-7(\alpha a+\beta b)=2a+3b$$

La réciproque en question est-elle vraie ?

1. Un simple développement donne :

$$6(2a+3b)-7(a+2b)=12a+18b-7a-14b=5a+4b$$

2. Supposons que 7 divise $2a+3b$ alors il divise divise tout multiple de $2a+3b$, en particulier il divise $6(2a+3b)$.
Par ailleurs, il est clair que 7 divise $7(a+2b)$.
Par différence, on en déduit que 7 divise $6(2a+3b)-7(a+2b)$ à savoir $5a+4b$.

3. Développons le membre de gauche :

$$30a+24b-7\alpha a-7\beta b=2a+3b$$

$$(30-7\alpha)a+(24-7\beta)b=2a+3b$$

Il suffit de choisir $30-7\alpha=2$, c'est-à-dire $\alpha=4$ et $24-7\beta=3$, c'est-à-dire $\beta=3$ ainsi on a :

$$6(5a+4b)-7(4a+3b)=2a+3b$$

On peut maintenant prouver que la réciproque est vraie. En effet, si 7 divise $5a+4b$ alors il divise la combinaison linéaire $6(5a+4b)-7(4a+3b)$ à savoir $2a+3b$.

Q 67 - Divisibilité et somme

[⋆⋆] [14%]

1. Soit $n\in\mathbb{N}^*$. Exprimer, en fonction de n, la somme suivante :

$$S_n=1+6+6^2+\cdots+6^{n-1}$$

2. En déduire que, pour tout $n\in\mathbb{N}$, 6^n+14 est un multiple de 5.

1. Il s'agit de la somme de n termes consécutifs d'une suite géométrique de raison $q=6$. On a donc :

$$S_n=\frac{1-q^n}{1-q}=\frac{1-6^n}{1-6}=\frac{6^n-1}{5}$$

2. Examinons déjà le cas $n=0$. Dans ce cas, $6^n+14=6^0+14=1+14=15$ et 15 est bien un multiple de 5.
Supposons maintenant $n\in\mathbb{N}^*$. On peut donc utiliser la question précédente qui nous permet d'affirmer que 6^n-1 est un multiple de 5 (puisqu'on peut écrire $6^n-1=5S_n$ et que S_n est un entier).
Il suffit maintenant d'écrire que $6^n+14=\left(6^n-1\right)+15$.
On vient de voir que 5 divise 6^n-1. Par ailleurs, 5 divise 15. Donc 5 divise la somme $\left(6^n-1\right)+15$ à savoir 6^n+14. En conclusion, 6^n+14 est toujours un multiple de 5.

Remarque

On peut retrouver ce résultat en utilisant les congruences :

$$6 \equiv 1\,[5]$$

Par élévation à la puissance n pour $n \in \mathbb{N}$:

$$6^n \equiv 1^n\,[5]$$

C'est-à-dire :

$$6^n \equiv 1\,[5]$$

D'où :

$$6^n + 14 \equiv 15 \equiv 0\,[5]$$

Ce qui signifie bien que $6^n + 14$ est un multiple de 5 pour tout $n \in \mathbb{N}$.

.....

Q 68 - VRAI ou FAUX sur la divisibilité

[⋆⋆] [19%]

Les nombres a, b et n ci-dessous sont des entiers naturels non nuls.

Pour chaque affirmation ci-dessous, dire si elle est vraie (et dans ce cas, la démontrer) ou fausse (et dans ce cas, donner un contre-exemple).

1. Si n divise $a+b$ et ab alors n divise a.

2. $n(n+1)$ est toujours un entier pair.

3. Il existe des entiers a et b tels que $3a + 12b = 22$.

4. Si a et b ont le même reste dans la division euclidienne par n alors $a - b$ est un multiple de n.

5. n et n^2 ont la même parité.

1. C'est FAUX. Voici un contre-exemple : 4 divise $2+6$ et 4 divise 2×6 mais pourtant 4 ne divise pas 2.

2. C'est VRAI. En effet, n et $n+1$ sont deux entiers consécutifs, dont l'un des deux est pair. Par conséquent le produit $n(n+1)$ est également pair. On peut également faire une preuve par récurrence :

- c'est vrai pour $n = 0$ car $0 \times 1 = 0$ ce qui est un nombre pair ;
- supposons $n(n+1)$ pair autrement dit n^2+n pair. Examinons $(n+1)(n+2)$ qui s'écrit $n^2+3n+2 = n^2+n+2n+2$. On constate que n^2+n est pair par hypothèse de récurrence. Mais $2n+2$ est également pair. Par conséquent, la somme $n^2+n+2n+2$ est paire. Donc $(n+1)(n+2)$ est un nombre pair. La propriété est ainsi initialisée et héréditaire, elle est donc vraie pour tout n.

3. C'est FAUX. En effet, $3a+12b$ peut s'écrire $3(a+4b)$. On voit ainsi qu'il s'agit d'un multiple de 3. Or, 22 n'est pas un multiple de 3. Il ne peut donc pas y avoir égalité entre $3a+12b$ et 22. (Lorsque a et b sont des entiers évidemment, sinon on peut prendre $a = \frac{1}{3}$ et $b = \frac{7}{4}$)

4. C'est VRAI. En effet, d'une part il existe un unique couple $(q\,,r)$ tel que :

$$a = nq + r \text{ avec } 0 \leqslant r < n$$

D'autre part, il existe un unique couple $(q'\,,r)$ tel que :

$$b = nq' + r \text{ avec } 0 \leqslant r < n$$

On en déduit que :

$$a - b = n(q - q')$$

Ce qui signifie bien que $a-b$ est un multiple de n.

5. C'est VRAI. On peut raisonner par disjonction des cas :

- Si n est pair, il peut s'écrire $n=2k$ où $k\in\mathbb{N}$. Dans ce cas, on a $n^2=(2k)^2=4k^2$ ce qui est un nombre pair ;
- Si n est impair, il peut s'écrire $n=2k+1$ où $k\in\mathbb{N}$. Dans ce cas, on a $n^2=(2k+1)^2=4k^2+4k+1$. Or $4k^2+4k$ est un nombre pair donc $4k^2+4k+1$ est un nombre impair.

En conclusion, n est n^2 ont bien la même parité.

.....

Q 69 - Utilisation d'une division euclidienne

[⋆⋆⋆] [15%]

Dans cet exercice, n désigne un entier relatif.

1. Quel est le reste de la division euclidienne de 25 par 4 ? Et de 36 par 4 ?

Démontrer que le reste de la division euclidienne de n^2 par 4 est toujours 0 ou 1.

2. Démontrer que le cube de tout entier relatif n est de la forme $9k$, $9k+1$ ou $9k+8$.

1. On a $25=4\times6+1$ donc le reste de la division euclidienne de 25 par 4 est 1.

On a $36=4\times9+0$ donc le reste de la division euclidienne de 36 par 4 est 0.

Procédons par disjonction des cas :

- si n est pair, alors il s'écrit $n=2k$ où $k\in\mathbb{Z}$. Dans ce cas, on a $n^2=4k^2=4\times k^2+0$ ce qui signifie que le reste de la division euclidienne de n^2 par 4 est 0 ;
- si n est impair, alors il s'écrit $n=2k+1$ où $k\in\mathbb{Z}$. Dans ce cas, on a $n^2=4k^2+4k+1=4(k^2+k)+1$ donc le reste de la division euclidienne de n^2 par 4 est 1.

Bilan : le reste de la division euclidienne de n^2 par 4 est toujours 0 ou 1.

2. Effectuons la division euclidienne de n par 3 :

$$n=3q+r \text{ avec } 0\leqslant r<3$$

Procédons par disjonction des cas :

- si $r=0$ alors $n^3=(3q)^3=27q^3=9\times3q^3=9k$ en choisissant $k=3q^3$;
- si $r=1$ alors $n^3=(3q+1)^3$. On rappelle ici l'identité remarquable suivante :

$$(A+B)^3=A^3+3A^2B+3AB^2+B^3$$

Et en particulier, lorsque $B=1$:

$$(A+1)^3=A^3+3A^2+3A+1$$

On a donc :

$$n^3=(3q+1)^3=27q^3+27q^2+9q+1=9(3q^3+3q^2+q)+1=9k+1$$

en choisissant $k=3q^3+3q^2+q$;

- si $r=2$ alors $n^3=(3q+2)^3$. L'identité remarquable précédente spécialisée avec $B=2$ donne :

$$(A+2)^3=A^3+6A^2+12A+8$$

On a donc :

$$n^3=(3q+2)^3=27q^3+54q^2+36q+8=9(3q^3+6q^2+4q)+8=9k+8$$

en choisissant $k=3q^3+6q^2+4q$.

Bilan : le reste de la division euclidienne de n^3 par 9 est toujours 0, 1 ou 8.

.....

Q 70 - Équation factorisable

[⋆] [31%]

Dans cet exercice, x et y désignent des entiers naturels.

1. Dresser la liste des diviseurs de 28

2. En utilisant une factorisation, en déduire la résolution de l'équation suivante :

$$x^2 - 9y^2 = 28$$

Combien de couples solutions obtient-on ?

1. Les diviseurs de 28 sont : 1, 2, 4, 7, 14, 28.

2. Factorisons l'équation :

$$(x - 3y)(x + 3y) = 28$$

Comme les facteurs $(x - 3y)$ et $(x + 3y)$ sont des entiers et compte-tenu du fait que $x - 3y$ est plus petit que $x + 3y$, nous avons donc les possibilités suivantes :

$$\begin{cases} x - 3y = 1 \\ x + 3y = 28 \end{cases} \quad \text{ou} \quad \begin{cases} x - 3y = 2 \\ x + 3y = 14 \end{cases} \quad \text{ou} \quad \begin{cases} x - 3y = 4 \\ x + 3y = 7 \end{cases}$$

Chacun de ces petits systèmes se résout facilement par addition ou soustraction.

En additionnant les deux lignes du premier système, on obtient $2x = 29$ ce qui est impossible car x est entier.

En additionnant les deux lignes du dernier système, on obtient $2x = 11$ ce qui est également impossible.

Seul le second système donne un couple solution. D'une part, en additionnant les deux lignes : $2x = 16$ d'où $x = 8$. D'autre part, en les soustrayant : $-6y = -12$ d'où $y = 2$.

On vérifie bien qu'alors $x^2 - 9y^2 = 8^2 - 9 \times 2^2 = 64 - 36 = 28$.

L'équation admet un seul couple solution, à savoir $(x\,,y) = (8\,,2)$.

.....

Q 71 - Équation de Pell-Fermat avec une infinité de solutions

[⋆⋆⋆] [31%]

On désigne par $(x\,,y)$ un couple d'entiers naturels solution de l'équation de Pell-Fermat suivante :

$$x^2 - 2y^2 = 1$$

1. Démontrer que x est nécessairement un entier impair. En déduire que y est nécessairement un entier pair.

2. Démontrer que x et y sont premiers entre-eux.

3. Vérifier que le couple $(x\,,y) = (1\,,0)$ est solution.
Démontrer que si le couple $(x\,,y)$ une solution quelconque de l'équation de Pell-Fermat alors le couple $(3x+4y\,,2x+3y)$ est également une solution de cette équation. En déduire deux nouveaux couples solution.

4. Écrire un algorithme qui permet de calculer et d'afficher n nouveaux couples solutions (n étant choisi par l'utilisateur) générés par cette méthode à partir du couple solution initial $(x\,,y) = (1\,,0)$.

1. On a $x^2 = 1 + 2y^2$. Bien sûr $2y^2$ est un entier pair, donc $1 + 2y^2$ est impair.
Donc x^2 est impair. Et comme un entier et son carré ont toujours la même parité, x est impair.
Puisque x est impair, on a donc $x = 2k + 1$ où $k \in \mathbb{N}$. L'équation de Pell-Fermat s'écrit alors :

$$(2k + 1)^2 - 2y^2 = 1$$

$$4k^2 + 4k + 1 - 2y^2 = 1$$

$$4(k^2+k) = 2y^2$$

$$2(k^2+k) = y^2$$

Donc y^2 est pair et, par conséquent, y aussi.

2. Soit d un diviseur commun de x et de y. Alors, d'après les propriétés de la divisibilité, d divise toute combinaison linéaire de x et de y donc, en particulier, d divise $x \times x - 2y \times y$ donc d divise $x^2 - 2y^2 = 1$. Donc $d = 1$. Les entiers x et y ont pour seul diviseur commun l'entier $d = 1$, ils sont donc premiers entre-eux.

Remarque

On peut également utiliser le théorème de Bézout puisqu'il existe un couple $(a\,,b)$ d'entiers tel que $ax + by = 1$. En effet, il suffit de choisir $a = x$ et $b = -2y$. On aboutit à la même conclusion.

3. On a $1^2 - 2 \times 0^2 = 1$ donc le couple $(1\,,0)$ est bien solution.

Supposons que $(x\,,y)$ soit un couple solution. On a donc $x^2 - 2y^2 = 1$.

Examinons ce qu'il en est alors pour le couple $(3x + 4y\,,2x + 3y)$:

$$(3x+4y)^2 - 2(2x+3y)^2 = 9x^2 + 24xy + 16y^2 - 8x^2 - 24xy - 18y^2 = x^2 - 2y^2 = 1$$

Le couple $(3x + 4y\,,2x + 3y)$ est donc, à son tour solution de l'équation.

On a donc un moyen de construire, de proche en proche, de nouveaux couples solutions.

En partant du couple $(1\,,0)$, on génère le couple $(3\times 1+4\times 0\,,2\times 1+3\times 0) = (3\,,2)$ puis ensuite vient le couple $(3 \times 3 + 4 \times 2\,,2 \times 3 + 3 \times 2) = (17\,,12)$. Et ainsi de suite, on peut construire une infinité de solutions.

4. Il s'agit de programmer le calcul des suites couplées suivantes

$$\begin{cases} x_0 = 1 \\ x_{n+1} = 3x_n + 4y_n \text{ pour tout } n \in \mathbb{N} \end{cases} \text{ et } \begin{cases} y_0 = 0 \\ y_{n+1} = 2x_n + 3y_n \text{ pour tout } n \in \mathbb{N} \end{cases}$$

On procède donc à l'aide d'une boucle « for ». Le problème est que si on saisit à la suite les deux instructions suivantes :

$$\text{X} \leftarrow \text{3*X+4*Y} \quad \text{et} \quad \text{Y} \leftarrow \text{2*X+3*Y}$$

le résultat pour la variable Y sera incorrect car calculé à partir de la nouvelle valeur de X et non de l'ancienne...

Il faut donc créer une variable temporaire T dans laquelle on stocke la variable X.

En langage Python, il n'y a pas ce problème car on peut faire des affectations de couple à couple !

Algorithme (langage naturel)

```
1.  VARIABLES
2.  X, Y, T, N, I SONT DU TYPE NOMBRE
3.  INITIALISATION
4.  X ← 1 ; Y ← 0
5.  DEBUT ALGORITHME
6.  AFFICHER « Nombre de couples souhaités »
7.  LIRE N
8.  POUR I ALLANT DE 1 A N
9.  DEBUT_POUR
10.   T ← X
11.   X ← 3*X+4*Y
12.   Y ← 2*T+3*Y
13.   AFFICHER X,Y
14. FIN_POUR
15. FIN ALGORITHME
```

Algorithme en Python

```
def Pell_Fermat(n) :
    x=1
    y=0
    for i in range(1,n+1) :          # pour i allant de 1 à n
        x, y = 3*x+4*y, 2*x+3*y      # calcul du nouveau couple (x_n , y_n)
        print(x,y)                   # afficher le couple (x , y)
```