Maths Expertes
Terminale

PGCD, Bézout & Gauss

CORRIGÉ DE L'EXERCICE

PGCD

10

Correction

Dans cet exercice, *a* et *b* s'expriment en fonction d'un entier $n \geq 5$ par :

$a = n^3 - n^2 - 12n$ et $b = 2n^2 - 7n - 4$.

Notons une factorisation évidente : $a = n(n^2 - n - 12)$.

Rappelons le lemme d'Euclide :

Si *a, b, q, r* sont des entiers relatifs non nuls tels que $a = bq + r$, alors $\mathrm{PGCD}(a\,;b) = \mathrm{PGCD}(b\,;r)$.

NB. Dans la **question 1**, nous aurons besoin de quelques propriétés des polynômes du second degré :

Soit $P(x) = ax^2 + bx + c$ un polynôme du second degré.

- Soit *u* un nombre réel ; *P* est factorisable par $(x - u)$ si et seulement si *u* est une racine de *P*, c'est-à-dire si et seulement si $P(u) = 0$.
- Si *P* admet deux racines x_1 et x_2, distinctes ou non, alors le produit des racines s'exprime en fonction des coefficients du polynôme : $x_1 \times x_2 = \frac{c}{a}$ (cette relation permet de calculer la deuxième racine quand l'une est connue).

1. Montrons que *a* et *b* sont des entiers naturels divisibles par $(n - 4)$:

Les nombres *a* et *b* sont des entiers relatifs en tant que cocktails (additions et multiplications) d'entiers relatifs.

Soit *X* et *Y* les polynômes du deuxième degré définis respectivement par :

$X(n) = n^2 - n - 12$ et $Y(n) = 2n^2 - 7n - 4$.

- $X(4) = Y(4) = 0$ ce qui signifie que 4 est une racine de chacun de ces polynômes. Ils sont donc l'un et l'autre factorisables par $(n - 4)$.
- Le produit des racines de *X* est égal à -12, la deuxième racine n_2 de ce polynôme est telle que $4 \times n_2 = -12$ donc $n_2 = -3$; ce polynôme est factorisable aussi par $(n + 3)$.

- Le produit des racines de Y est $\frac{-4}{2} = -2$, la deuxième racine n'_2 de ce polynôme est telle que $4 \times n'_2 = -2$ donc $n'_2 = -\frac{1}{2}$; ce polynôme est factorisable aussi par $\left(n + \frac{1}{2}\right)$. Le coefficient de x^2 étant égal à 2, ce polynôme est donc factorisable par le monôme à coefficients entiers : $2 \times \left(n + \frac{1}{2}\right) = (2n + 1)$.

Ce qui conduit aux factorisations :

$X(n) = (n - 4)(n + 3)$; $Y(n) = 2(n - 4)\left(n + \frac{1}{2}\right) = (n - 4)(2n + 1)$

Nous en déduisons des décompositions en produit de facteurs des entiers a et b :

$$a = nX(n) = n(n - 4)(n + 3)$$

$$b = Y(n) = (n - 4)(2n + 1)$$

NB. L'hypothèse $n \geq 5$ garantit que l'entier $n - 4$ est un entier strictement positif. Il apparaît au vu des factorisations que tous les autres facteurs sont aussi des entiers strictement positifs ; les entiers a et b sont toujours deux entiers strictement positifs.

2.a. Montrons que $\mathrm{PGCD}(\alpha\ ;\ \beta)$ divise 5 :

Cherchons une relation indépendante de n entre α et β : $\begin{cases} 2\beta = 2n + 6 \\ \alpha = 2n + 1 \end{cases} \Rightarrow \alpha = 2\beta - 5$.

Il s'agit d'une combinaison entière de α et β à laquelle nous pouvons appliquer le lemme d'Euclide avec les paramètres $\alpha = a$; $\beta = b$; $q = 2$; $r = -5$:

$$\text{PGCD}(\alpha\ ;\ \beta) = \text{PGCD}(\beta\ ;\ -5) = \text{PGCD}(\beta\ ;\ 5)$$

Il en résulte que : $\text{PGCD}(\alpha\ ;\ \beta)$ divise 5.

NB. Nous en déduisons que ce PGCD est égal ou bien à 1 ou bien à 5 puisque 5 est un nombre premier.

2.b. Montrons que si α et β sont multiples de 5, alors $n - 2 \equiv 0\ [5]$:

Supposons que α et β soient des multiples de 5. En termes de congruences, cette propriété se traduit par : $\begin{cases} \alpha \equiv 0\ [5] \\ \beta \equiv 0\ [5] \end{cases}$ soit $\begin{cases} 2n + 1 \equiv 0\ [5] \\ n + 3 \equiv 0\ [5] \end{cases}$. Nous obtenons une nouvelle congruence modulo 5 en retranchant membre à membre ces deux congruences :

$$\begin{cases} \alpha \equiv 0\ [5] \\ \beta \equiv 0\ [5] \end{cases} \Rightarrow (2n + 1) - (n + 3) \equiv 0\ [5]$$

Nous obtenons : $\begin{cases} \alpha \equiv 0\ [5] \\ \beta \equiv 0\ [5] \end{cases} \Rightarrow n - 2 \equiv 0\ [5]$

Si α et β sont multiples de 5, alors $n - 2 \equiv 0\ [5]$.

NB. Réciproquement, si $n-2 \equiv 0\ [5]$, alors $\beta = n+3 \equiv 0\ [5]$, $\mathrm{PGCD}(\alpha\,;\,\beta) = \mathrm{PGCD}(\beta\,;5) = 5$.

Il y a donc en fait équivalence : $\begin{cases} \alpha \equiv 0\ [5] \\ \beta \equiv 0\ [5] \end{cases} \Leftrightarrow\ n-2 \equiv 0\ [5]$.

L'implication demandée par l'énoncé démontre par contraposition que, si $n-2 \not\equiv 0\ [5]$, alors α et β ne sont pas deux multiples de 5, donc que dans ce cas leur PGCD est nécessairement égal à 1.

3. Montrons que α et *n* sont premiers entre eux :

Nous avons : $\alpha - 2n = (2n+1) - 2n = 1$

La relation $\alpha - 2n = 1$ est une relation de Bézout qui montre que α et *n* sont premiers entre eux.

4.a. Déterminons le PGCD de *a* et de *b* :

Il s'agit de déterminer le PGCD de $a = n(n-4)(n+3)$ et de $b = (n-4)(2n+1)$.

Ces nombres étant tous deux multiples de l'entier strictement positif $(n-4)$:

$$\mathrm{PGCD}(a\,;b) = (n-4) \times \mathrm{PGCD}(n(n+3)\ ;\ 2n+1)$$

Les deux entiers *n* et $2n+1$ étant premiers entre eux,

$$\mathrm{PGCD}(n(n+3)\ ;\ 2n+1) = \mathrm{PGCD}(n+3\ ;\ 2n+1)$$

En définitive : $\mathrm{PGCD}(a\,;b) = (n-4) \times \mathrm{PGCD}(\alpha\,;\,\beta)$

Compte tenu des résultats de la **question 2** :

- Si $n \equiv 2\ [5]$ alors $\mathrm{PGCD}(a\,;b) = 5(n-4)$
- $\text{Sinon, } \mathrm{PGCD}(a\,;b) = n-4$

4.b. Vérifions (avec Python) :

<table>
<tr>
<td>Nous reconnaissons dans le PGCD de a et de b l'entier $(n-4)$ qui est quintuplé lorsque n est égal à 7 ou à 12.
Seules les lignes 11 et 12 sont exigées par l'énoncé.</td>
<td>

```
>>> from math import gcd
>>> def pgcd10():
        for n in range(5,13):
                a=n**3-n**2-12*n
                b=2*(n**2)-7*n-4
                d=gcd(a,b)
                print("si n=",n,"a=",a,"b=",b,"etPGCD(a,b)=",d)


>>> pgcd10()
si n= 5 a= 40 b= 11 etPGCD(a,b)= 1
si n= 6 a= 108 b= 26 etPGCD(a,b)= 2
si n= 7 a= 210 b= 45 etPGCD(a,b)= 15
si n= 8 a= 352 b= 68 etPGCD(a,b)= 4
si n= 9 a= 540 b= 95 etPGCD(a,b)= 5
si n= 10 a= 780 b= 126 etPGCD(a,b)= 6
si n= 11 a= 1078 b= 161 etPGCD(a,b)= 7
si n= 12 a= 1440 b= 200 etPGCD(a,b)= 40
```

</td>
</tr>
</table>