www.freemaths.fr

Maths Expertes
Terminale

PGCD, Bézout & Gauss

CORRIGÉ DE L'EXERCICE

GAUSS

08

Correction

NB. Cet exercice propose un exemple du « **théorème chinois** » qui s'énonce en termes de congruences ainsi : « Soit *a* et *b* des entiers premiers entre eux. Quel que soit α et β entiers, il existe des entiers *n* solutions des congruences simultanées $\begin{cases} n \equiv \alpha \ \ (a) \\ n \equiv \beta \ \ (b) \end{cases}$ et ces solutions sont congrues entre elles modulo $a \times b$ ».

Rappelons pour la **question 1** le théorème de Bézout : « deux entiers relatifs *a* et *b* sont premiers entre eux si et seulement s'il existe des entiers *u* et *v* vérifiant $ua + vb = 1$ »

1.Recherche d'un élément de $\mathcal{S}$:

1.a. Justifions l'existence d'un couple $(u,\ v)$ tel que $17u + 5v = 1$:

Nous savons que deux nombres premiers distincts sont toujours premiers entre eux. Or, 17 et 5 sont deux nombres premiers distincts. 17 et 5 sont donc premiers entre eux, nous pouvons leur appliquer le théorème de Bézout :

Il existe au moins un couple d'entiers relatifs $(u,\ v)$ tel que $17u + 5v = 1$.

1.b. Vérifions qu'alors $n_0 = 3 \times 17u + 9 \times 5v$ appartient à $\mathcal{S}$:

Soit $(u,\ v)$ un couple d'entiers relatifs tel que $17u + 5v = 1$. (Nous venons de prouver l'existence d'au moins un tel couple). Ces entiers *u* et *v*, du fait qu'ils vérifient la relation $17u + 5v = 1$, possèdent la particularité suivante :

- Si nous utilisons une congruence modulo 17 : $5v - 1 = -17u \implies 5v \equiv 1 \ \ (17)$.
- Si nous utilisons une congruence modulo 5 : $17u - 1 = -5v \implies 17u \equiv 1 \ \ (5)$.

Soit $n_0 = 3 \times 17u + 9 \times 5v$.

Utilisons à propos de ce nombre une congruence modulo 17 et une congruence modulo 5 :

- $n_0 \equiv 9 \times 5v \ (17)$ car $n_0 - 9 \times 5v = 3 \times 17u$ est un multiple de 17.
- $n_0 \equiv 3 \times 17u \ (5)$ car $n_0 - 3 \times 17u = 9 \times 5v$ est un multiple de 5.

En vertu de la compatibilité des congruences modulo 17 et modulo 5 avec la multiplication :

- $5v \equiv 1 \ (17) : \implies n_0 \equiv 9 \ (17)$.
- $17u \equiv 1 \ (5) : \implies n_0 \equiv 3 \ (5)$.

L'entier n_0 vérifie simultanément les deux congruences en jeu, il appartient à $\mathcal{S}$.

1.c. Donnons un exemple d'entier appartenant à $\mathcal{S}$:

Pour cela, proposons une solution particulière de l'équation $17u + 5v = 1$ en saisissant l'opportunité d'une solution « évidente » :

$$35 = 5 \times 7 = 34 + 1 = 17 \times 2 + 1$$

Ainsi nous disposons de l'égalité stratégique : $\mathbf{17 \times (-2) + 5 \times 7 = 1.}$

Le couple $(u_0 = -2, \ v = 7)$ est solution particulière de l'équation $17u + 5v = 1$.

Considérons alors l'entier : $n_0 = 3 \times 17 \times (-2) + 9 \times 5 \times 7 = -102 + 315 = 213$.

- D'une part : $213 = 17 \times 12 + 9$ donc $213 \equiv 9 \ (17)$
- D'autre part : $213 = 5 \times 42 + 3$ donc $213 \equiv 3 \ (5)$

L'entier 213 est un exemple d'élément de $\mathcal{S}$.

2. Caractérisation des éléments de $\mathcal{S}$:

2.a. Montrons que si *n* appartient à $\mathcal{S}$, alors $n - n_0 \equiv 0 \ (85)$:

NB. Dans cette question, n_0 représente un élément particulier de l'ensemble $\mathcal{S}$, par exemple l'entier 213 que nous avons proposé à la question précédente. Retenons seulement que cet élément particulier, quel qu'il soit, est congru à 9 modulo 17 et à 3 modulo 5.

Rappelons qu'étant donné deux congruences de même modulo *p*, nous obtenons une nouvelle congruence modulo *p* en retranchant membre à membre les deux congruences.

Soit *n* un élément quelconque de $\mathcal{S}$. Confrontons ses propriétés avec celles de l'élément particulier n_0.

- Modulo 17 : $\begin{cases} n \equiv 9 \ (17) \\ n_0 \equiv 9 \ (17) \end{cases} \Rightarrow \ n - n_0 \equiv 0 \ (17)$
- Modulo 5 : $\begin{cases} n \equiv 3 \ (5) \\ n_0 \equiv 3 \ (5) \end{cases} \Rightarrow \ n - n_0 \equiv 0 \ (5)$

L'entier $(n - n_0)$ est congru à 0 à la fois modulo 17 et modulo 5. Il s'agit donc à la fois d'un multiple de 17 et d'un multiple de 5, par conséquent d'un multiple de leur PPCM. Or, les entiers 5 et 17 sont des entiers premiers entre eux, leur PPCM est égal à leur produit, le nombre $17 \times 5 = 85$.

Si *n* appartient à $\mathcal{S}$, alors le nombre $(n - n_0)$ est un multiple de 85, autrement dit :

$$n - n_0 \equiv 0 \ (85)$$

2.b. Montrons que *n* appartient à $\mathcal{S}$ si et seulement si n est de la forme $n = 43 + 85k$:

NB. Il nous reste à choisir numériquement un élément particulier n_0. Nous avons proposé l'entier 213, trouvé à la **question 1.c**, mais l'énoncé nous impose l'entier 43.

.

Remarquons que $\begin{cases} 43 = 2 \times 17 + 9 \\ 43 = 5 \times 8 + 3 \end{cases}$ donc $\begin{cases} 43 \equiv 9 \ (17) \\ 43 \equiv 3 \ (5) \end{cases}$. L'entier 43 appartient à $\mathcal{S}$. Il s'agit bien d'un élément particulier de $\mathcal{S}$, au même titre que 213, dont il diffère d'un multiple de 85 (en effet, leur différence est $213 - 43 = 170 = 2 \times 85$). Choisissons donc désormais : $n_0 = 43$.

D'après le résultat de la **question 2.a**, si *n* appartient à $\mathcal{S}$, alors $n - 43 \equiv 0 \ (85)$, c'est-à-dire qu'il existe un entier relatif *k* tel que $n = 43 + 85k$.

Réciproquement, soit *n* un entier tel qu'il existe un entier relatif *k* vérifiant $n = 43 + 85k$.

Alors : $\begin{cases} n = 9 + (34 + 85k) = 9 + 17 \times (2 + 5k) \\ n = 3 + (40 + 85k) = 3 + 5 \times (8 + 17k) \end{cases}$ donc $\begin{cases} n \equiv 9 \ (17) \\ n \equiv 3 \ (5) \end{cases}$. L'entier *n* appartient à $\mathcal{S}$.

Bilan : La **question 2.a** montre que $\mathcal{S} \subset \{43 + 85k, \ k \in \mathbb{Z}\}$ et la réciproque ci-dessus montre que, inversement, $\mathcal{S} \supset \{43 + 85k, \ k \in \mathbb{Z}\}$. Il y a égalité entre les deux ensembles.

Un entier *n* appartient à $\mathcal{S}$ si et seulement s'il existe un entier relatif *k* vérifiant $n = 43 + 85k$.

L'ensemble $\mathcal{S}$ est l'ensemble $\{43 + 85k, \ k \in \mathbb{Z}\}$.