Algèbre
Arithmétique

Denis Vekemans *

Solution 4 D'après le théorème de Bézout,

$$\exists u \in \mathbb{Z},\ \exists v \in \mathbb{Z} \text{ tels que } au + bv = 1.$$

On déduit $\exists u \in \mathbb{Z}, \exists v \in \mathbb{Z}$ tels que $auc + bvc = c$, mais a divise auc et comme a divise bc, a divise bvc, puis a divise c.

Solution 5 D'après le théorème de Bézout,

$$\exists u \in \mathbb{Z},\ \exists v \in \mathbb{Z} \text{ tels que } bu + cv = 1.$$

Comme b divise a, $\exists d \in \mathbb{Z}$ tel que $db = a$ et comme c divise a, $\exists e \in \mathbb{Z}$ tel que $ec = a$. De $\exists u \in \mathbb{Z}, \exists v \in \mathbb{Z}$ tels que $bu + cv = 1$, on déduit $\exists u \in \mathbb{Z}, \exists v \in \mathbb{Z}$ tels que $abu + acv = a$, puis $\exists u \in \mathbb{Z}, \exists v \in \mathbb{Z}, \exists d \in \mathbb{Z}, \exists e \in \mathbb{Z}$ tels que $ecbu + dbcv = a$ ou $bc(eu + dv) = a$, puis bc divise a.

Solution 6 On débute par un **lemme** : "soit a le $PGCD$ de b et de c, alors tout diviseur commun à b et à c est diviseur de a".

C'est une propriété qui provient directement de la décomposition d'un entier en produit de facteurs premiers : soit p_i le $i$ème nombre premier, on a $b = \sigma_b \prod_i p_i^{\beta_i}$ (avec $\beta_i \in \mathbb{N}$ et $\sigma_b \in \{-1, +1\}$) et $c = \sigma_c \prod_i p_i^{\gamma_i}$ (avec $\gamma_i \in \mathbb{N}$ et $\sigma_c \in \{-1, +1\}$), puis $a = \prod_i p_i^{\min(\beta_i, \gamma_i)}$ et tout diviseur commun à b et à c s'écrit sous la forme $\sigma_d \prod_i p_i^{\delta_i}$ où $\delta_i \in \mathbb{N}$ tel que $\delta_i \leq \min(\beta_i, \gamma_i)$ et où $\sigma_d \in \{-1, +1\}$, puis divise a.

■

Soit d le $PGCD$ de a et c. Soit d' le $PGCD$ de a et bc.

– On montre que d divise d'.
Par définition du $PGCD$, d divise a et d divise c, donc d divise a et d divise bc, donc d divise d' (d'après le lemme).

*Laboratoire de mathématiques pures et appliquées Joseph Liouville ; 50, rue Ferdinand Buisson BP 699 ; 62 228 Calais cedex ; France

– On montre que d divise d'.

Préalablement, on montre que le $PGCD$ de d' et b est 1 : le $PGCD$ de d' et b divise d' et b par définition du $PGCD$, donc divise a et b car d' divise a, donc divise le $PGCD(a,b)$ (d'après le lemme) qui est 1, donc le $PGCD$ de d' et b ne peut être que 1.

Maintenant, par définition du $PGCD$, d' divise a et d' divise bc, donc d' divise a et d' divise c (d'après le théorème de Gauss qui est applicable car le $PGCD$ de d' et b est 1), donc d' divise d (d'après le lemme).

Solution 10 Soit d tel que d divise 2^n+1 et d divise $2^{n+1}+1$. Alors d divise $-(2^{n+1}+1)+2(2^n+1)=1$. Donc le $PGCD$ de 2^n+1 et $2^{n+1}+1$ ne peut être que 1.

Solution 12 m divise $(m-1)!+1$.

Si m n'est pas premier, soit d un de ses diviseurs positifs distinct de 1 et de m.

Ainsi, d'une part d divise m et $d<m$, donc d divise $(m-1)!$. Et d'autre part, d divise m, donc d divise $(m-1)!+1$.

De ces deux conclusions, on tire que d divise $(m-1)!+1-(m-1)!=1$, puis $d=1$, ce qui est absurde.

Solution 13 Si m n'est pas premier, soit d un de ses diviseurs positifs distinct de 1 et de m.

On a alors $m=dd'$ avec d' un des diviseurs positifs de m distinct de 1 et de m.

Puis, $2^m-1=2^{dd'}-1=(2^d-1)(2^{d(d'-1)}+2^{d(d'-2)}+\ldots+2^d+1)$.

Mais comme $d\neq 1$, $2^d-1\neq 1$ et comme $d\neq m$, $2^d-1\neq 2^m-1$. Donc 2^d-1 est un diviseur positif de 2^m-1 distinct de 1 et de 2^m-1, puis 2^m-1 n'est pas premier, ce qui est absurde.

Solution 14 On effectue la division euclidienne du polynôme en n n^3+n par le polynôme en n $2n+1$. On trouve un quotient égal à $\frac{n^2}{2}-\frac{n}{4}+\frac{5}{8}$ et un reste égale à $\frac{-5}{8}$.

On déduit donc

$$-8(n^3+n)+(2n+1)(4n^2-2n+5)=5.$$

D'après le théorème de Bézout, le $PGCD$ de n^3+n et $2n+1$ est donc soit 1 soit 5 (car il divise 5).

Premier cas : $2n+1$ est multiple de 5.

Dans ce cas, $2n+1=5m$ avec $m\in\mathbb{Z}$, mais comme un nombre impair ne peut être produit dans $\mathbb{Z}$ que de deux nombres impairs, on a $m=2k+1$ avec $k\in\mathbb{Z}$. Ainsi, $2n+1=10k+5$, puis $n=5k+2$. Ensuite, $n^3+n=(5k+2)^3+(5k+2)=125k^3+150k^2+65k+10=5(25k^3+30k^2+13k+2)$ et n^3+n est divisible par 5.

$2n+1$ et n^3+n sont tous deux divisibles par 5, donc le $PGCD$ de n^3+n et $2n+1$ est multiple de 5, mais comme le $PGCD$ de n^3+n et $2n+1$ est aussi diviseur de 5, le $PGCD$ de n^3+n et $2n+1$ est égal à 5.

Deuxième cas : $2n+1$ n'est pas multiple de 5.

Dans ce cas, 5 ne peut être $PGCD$ de $2n+1$ (puisqu'il n'est même pas diviseur de $2n+1$) et n^3+n. Il s'ensuit que le $PGCD$ de n^3+n et $2n+1$ (qui ne pouvait être que 1 ou 5) est 1.

Solution 17

1. $$\phi(m) = \#\{d \leq m \text{ tels que le } PGCD \text{ de } d \text{ et } m \text{ soit } 1\}.$$

   D'après le théorème de Bézout,

   $$\exists u \in \mathbb{Z},\ \exists v \in \mathbb{Z} \text{ tels que } du + mv = 1.$$

   On déduit que $du \equiv 1 \mod (m)$, puis que d est inversible (d'inverse $d^{-1} = u$) dans $\mathbb{Z}/m\mathbb{Z}$.

2. $\phi(mn)$ est le nombre d'éléments inversibles de $\mathbb{Z}/mn\mathbb{Z}$ qui est isomorphe à $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (voir exercice sur les anneaux et corps) dont le nombre d'éléments inversibles est $\phi(m)\phi(n)$ (i.e. pour représenter x dans $\mathbb{Z}/mn\mathbb{Z}$, on peut le noter $\bar{x}$ qui est la classe de x dans $\mathbb{Z}/mn\mathbb{Z}$, mais d'après l'isomorphisme, il est équivalent de le représenter dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ par un couple $(\widehat{x}, \widetilde{x})$ où $\widehat{x}$ est la classe de x dans $\mathbb{Z}/m\mathbb{Z}$ et où $\widetilde{x}$ est la classe de x dans $\mathbb{Z}/n\mathbb{Z}$, puis dire que $\bar{x}$ est inversible d'inverse $\bar{x}^{-1}$ c'est dire que $(\widehat{x}, \widetilde{x})$ est inversible d'inverse $(\widehat{x}, \widetilde{x})^{-1} = (\widehat{x}^{-1}, \widetilde{x}^{-1})$).

3. Si $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, d'après la question précédente, $\phi(m) = \phi(p_1^{\alpha_1}) \dots \phi(p_k^{\alpha_k})$.

   Mais, si p est un nombre premier, on a

   $$\begin{aligned} \phi(p^\alpha) &= \underbrace{p^\alpha}_{\substack{\text{nombre d'éléments inférieurs à } p^\alpha}} \\ &- \Big(\underbrace{p^{\alpha-1}}_{\substack{\text{nombre d'éléments de d'éléments inférieurs à } p^\alpha \text{ non premiers avec } p^\alpha}} \Big) . \end{aligned}$$

   Remarque : les éléments non premiers avec p^α ont p en facteur ...

   Puis,

   $$\phi(p^\alpha) = p^\alpha(1 - \frac{1}{p}).$$

   Et, enfin,

   $$\phi(m) = \underbrace{p_1^{\alpha_1} \dots p_k^{\alpha_k}}_{=m}(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}).$$