Problèmes type Bac & Solutions : Arithmétique

Mohamed Kadhem Karray
https://mohamedkadhem.com/baccalaureat/

Dans les solutions, un renvoi comme *Théorème 16.11 du cours 16* désigne un énoncé numéroté du cours 16 [1], sur l'arithmétique. Le numéro entre crochets renvoie à la bibliographie en fin de document. Ce cours est disponible sur la page `mohamedkadhem.com/baccalaureat`.

Problème 1 *Dans ce problème, on utilise les congruences, l'algorithme d'Euclide, le théorème de Bézout et le petit théorème de Fermat.*

Partie A : congruences

1. *Montrer que, pour tout* $n \in \mathbb{Z}$*, le nombre* n^2+n+3 *est impair.*
2. *Déterminer les entiers* $n \in \mathbb{Z}$ *tels que* n^2+2n+3 *soit divisible par* 5*.*

Partie B : inverse modulo 13 ***et petit théorème de Fermat***

1. (a) *Calculer* $\text{PGCD}(13,5)$ *par l'algorithme d'Euclide.*
   (b) *En remontant les divisions de la question (a), trouver deux entiers* u *et* v *tels que* $13u+5v=1$*.*
   (c) *En déduire un inverse de* 5 *modulo* 13*, compris entre* 0 *et* 12*.*
2. *Montrer que* 13 *est un nombre premier. En déduire que* $3^{12} \equiv 1\,[13]$*, et que* $n^{13}-n$ *est divisible par* 13 *pour tout* $n \in \mathbb{Z}$*.*
3. *Déterminer le reste de la division euclidienne de* 3^{100} *par* 13*.*
4. *Déterminer les entiers* $x \in \mathbb{Z}$ *tels que* $5x \equiv 3^{100}\,[13]$*.*

Solution 1 ***Partie A : congruences***

1. *Pour tout* $n \in \mathbb{Z}$*, on a* $n^2+n+3 = n(n+1)+3$*. Par le Théorème 16.3 (ii) du cours 16 [1], avec* $b=2$*, l'entier* n *s'écrit* $n=2q$ *ou* $n=2q+1$*, avec* $q \in \mathbb{Z}$*.*
   - *Si* $n=2q$*, alors* $n(n+1) = 2[q(2q+1)]$*.*
   - *Si* $n=2q+1$*, alors* $n(n+1) = (2q+1)(2q+2)$*, soit* $n(n+1) = 2[(2q+1)(q+1)]$*.*

Dans les deux cas, $n(n+1) = 2m$ avec $m \in \mathbb{Z}$, donc $n^2+n+3 = 2m+3 = 2(m+1)+1$: ce nombre est impair.

2. *Soit $n \in \mathbb{Z}$, et soit $N = n^2 + 2n + 3$. Par le Théorème 16.3 (ii) du cours 16 [1], avec $b = 5$, l'entier n s'écrit $n = 5q + r$, avec $q \in \mathbb{Z}$ et $r \in \{0, 1, 2, 3, 4\}$; cela vaut aussi pour n négatif. Alors $n - r = 5q$, c'est-à-dire $n \equiv r\,[5]$ (Définition 16.3 du cours 16 [1]). Le Théorème 16.5 (iii), (ii) et (i) du cours 16 [1] donne alors*

$$N \equiv r^2 + 2r + 3\,[5]\,.$$

On calcule $r^2 + 2r + 3$ pour chaque valeur de r :

r	0	1	2	3	4
r^2+2r+3	3	6	11	18	27
reste par 5	3	1	1	3	2

car $6 = 5+1$, $11 = 5\times2+1$, $18 = 5\times3+3$ et $27 = 5\times5+2$. Dans chaque cas, le reste s de $r^2 + 2r + 3$ par 5 appartient à $\{1, 2, 3\}$, et le Théorème 16.4 (ii) du cours 16 donne $r^2+2r+3 \equiv s\,[5]$; donc $N \equiv s\,[5]$ (Théorème 16.4 (iii) du cours 16 [1]). Comme $0 \leq s \leq 4$, le Théorème 16.4 (ii) du cours 16 [1] dit que s est le reste de la division euclidienne de N par 5. Ce reste n'est pas nul, donc $5 \nmid N$ (Théorème 16.3 (i) du cours 16 [1]).

Ainsi, $n^2 + 2n + 3$ n'est divisible par 5 pour aucun entier n : l'ensemble cherché est vide.

Partie B : inverse modulo 13 *et petit théorème de Fermat*

1. (a) *On applique l'algorithme d'Euclide à 13 et 5, qui sont dans $\mathbb{N}^*$:*

$$\begin{aligned} 13 &= 5 \times 2 + 3, \\ 5 &= 3 \times 1 + 2, \\ 3 &= 2 \times 1 + 1, \\ 2 &= 1 \times 2 + 0. \end{aligned}$$

Le dernier reste non nul est 1 ; par le Théorème 16.7 (iii) du cours 16, $\mathrm{PGCD}(13, 5) = 1$, donc 13 et 5 sont premiers entre eux (Définition 16.5 du cours 16 [1]).

(b) *Comme dans l'Exemple 16.7 du cours 16 [1], on exprime chaque reste à partir des deux précédents, en partant du dernier reste non nul :*

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = 2 \times 3 - 5 \\ &= 2 \times (13 - 2 \times 5) - 5 = 2 \times 13 - 5 \times 5. \end{aligned}$$

Donc $(u, v) = (2, -5)$ convient. Vérification : $13 \times 2 + 5 \times (-5) = 26 - 25 = 1$.

(c) *Par la question (b),* $5 \times (-5) = 1 - 13 \times 2$*, donc, par la Définition 16.3 du cours 16,* $5 \times (-5) \equiv 1\,[13]$ *:* -5 *est un inverse de* 5 *modulo* 13 *(Corollaire 16.3 du cours 16 [1], avec* $n = 13 \geq 2$*). De plus* $-5 \equiv 8\,[13]$*, car* $8 - (-5) = 13$*, donc* $5 \times 8 \equiv 5 \times (-5) \equiv 1\,[13]$ *(Théorème 16.5 (ii) et Théorème 16.4 (iii) du cours 16 [1]). Ainsi* 8 *est un inverse de* 5 *modulo* 13 *compris entre* 0 *et* 12*. Vérification :* $5 \times 8 = 40 = 13 \times 3 + 1$*.*

2. *Par la Remarque 16.8 du cours 16 [1], il suffit de tester les nombres premiers* p *tels que* $p^2 \leq 13$*, c'est-à-dire* 2 *et* 3 *(car* $5^2 = 25 > 13$*). Or* $13 = 2 \times 6 + 1$ *et* $13 = 3 \times 4 + 1$ *: ni* 2 *ni* 3 *ne divise* 13 *(Théorème 16.3 (i) du cours 16 [1]). Donc* 13 *est premier.*

   Comme $3 \neq 0$ *et* $3 < 13$*, l'entier* 13 *ne divise pas* 3 *(Théorème 16.1 (iv) du cours 16 [1]). Comme* 13 *est premier et que* $13 \nmid 3$*, le Théorème 16.18 (i) du cours 16 [1] donne* $3^{13-1} = 3^{12} \equiv 1\,[13]$*.*

   Pour tout $n \in \mathbb{Z}$*, le Théorème 16.18 (ii) du cours 16 donne* $n^{13} \equiv n\,[13]$*, c'est-à-dire* $13 \mid n^{13} - n$ *(Définition 16.3 du cours 16 [1]).*

3. *On divise l'exposant par* 12 *:* $100 = 12 \times 8 + 4$*, donc* $3^{100} = \left(3^{12}\right)^8 \times 3^4$*. Par la question 2 et le Théorème 16.5 (iii) puis (ii) du cours 16 [1], on en déduit* $3^{100} \equiv 1^8 \times 3^4 = 81\,[13]$*. Or* $81 = 13 \times 6 + 3$*, donc* $81 \equiv 3\,[13]$*, et* $3^{100} \equiv 3\,[13]$ *(Théorème 16.4 (iii) du cours 16 [1]). Comme* $0 \leq 3 < 13$*, le reste de la division euclidienne de* 3^{100} *par* 13 *est* 3 *(Théorème 16.4 (ii) du cours 16 [1]).*

   Contrôle : $3^3 = 27 = 13 \times 2 + 1$*, donc* $3^3 \equiv 1\,[13]$ *; avec* $100 = 3 \times 33 + 1$*, on obtient de même* $3^{100} = \left(3^3\right)^{33} \times 3 \equiv 3\,[13]$*.*

4. *Par la question 3,* $3^{100} \equiv 3\,[13]$*. Par le Théorème 16.4 (iii) du cours 16 [1],* $5x \equiv 3^{100}\,[13]$ *si et seulement si* $5x \equiv 3\,[13]$*.*

   Supposons $5x \equiv 3\,[13]$*. En multipliant par l'inverse* 8 *de la question 1 (c), on obtient* $40x \equiv 24\,[13]$ *(Théorème 16.5 (ii) du cours 16 [1]). Or* $40 \equiv 1\,[13]$*, donc* $40x \equiv x\,[13]$*, et* $24 = 13 + 11$*, donc* $24 \equiv 11\,[13]$*. Par le Théorème 16.4 (iii) du cours 16 [1],* $x \equiv 11\,[13]$*.*

   Réciproquement, si $x \equiv 11\,[13]$*, alors* $5x \equiv 55\,[13]$ *(Théorème 16.5 (ii) du cours 16 [1]), et* $55 = 13 \times 4 + 3$*, donc* $5x \equiv 3\,[13]$*.*

   Les entiers cherchés sont donc les entiers $x \equiv 11\,[13]$*, c'est-à-dire l'ensemble* $\{11 + 13k : k \in \mathbb{Z}\}$*.*

Problème 2 *On considère dans* $\mathbb{Z}^2$ *l'équation*

$$(E) : \quad 5x - 12y = 1.$$

1. (a) *Calculer* $\mathrm{PGCD}\,(12, 5)$ *par l'algorithme d'Euclide, et en déduire que l'équation* (E) *a des solutions.*

(b) *En remontant les divisions de la question (a), trouver une solution particulière de* (E).

(c) *Résoudre l'équation* (E) *dans* $\mathbb{Z}^2$.

2. *En déduire les entiers* $n \in \mathbb{Z}$ *tels que* $5n \equiv 1\,[12]$, *et le plus petit d'entre eux qui est strictement positif.*

3. (a) *Montrer que* 13 *est un nombre premier.*

(b) *Montrer que, pour tout* $a \in \mathbb{Z}$ *et tout* $m \in \mathbb{N}$, $a^{12m+1} \equiv a\,[13]$.

4. *Soit* $n \in \mathbb{N}$ *tel que* $5n \equiv 1\,[12]$. *Montrer que, pour tout* $a \in \mathbb{Z}$, $a^{5n} \equiv a\,[13]$.

5. (a) *Montrer que, si* $x \in \mathbb{Z}$ *vérifie* $x^5 \equiv 2\,[13]$, *alors* $x \equiv 2^5\,[13]$.

(b) *En déduire les entiers* $x \in \mathbb{Z}$ *tels que* $x^5 \equiv 2\,[13]$.

Solution 2 1. (a) *On applique l'algorithme d'Euclide à* 12 *et* 5, *qui sont dans* $\mathbb{N}^*$:

$$12 = 5 \times 2 + 2,$$
$$5 = 2 \times 2 + 1,$$
$$2 = 1 \times 2 + 0.$$

Le dernier reste non nul est 1, *donc* $\mathrm{PGCD}\,(12, 5) = 1$ *(Théorème 16.7 (iii) du cours 16 [1]). Par la Remarque 16.4 (i) du cours 16 [1],* $\mathrm{PGCD}\,(5, -12) = \mathrm{PGCD}\,(5, 12) = 1$.

L'équation (E) *s'écrit* $ax + by = c$ *avec* $a = 5$ *et* $b = -12$, *non nuls, et* $c = 1$. *Comme* $1 \mid 1$, *elle a des solutions (Théorème 16.12 (i) du cours 16 [1]).*

(b) *Comme dans l'Exemple 16.7 du cours 16 [1], on remonte les divisions de la question (a) :*

$$1 = 5 - 2 \times 2 = 5 - 2 \times (12 - 5 \times 2) = 5 \times 5 - 2 \times 12.$$

Donc $5 \times 5 - 12 \times 2 = 1$ *: le couple* $(x_0, y_0) = (5, 2)$ *est une solution particulière de* (E). *Vérification :* $25 - 24 = 1$.

(c) *Ici* $d = \mathrm{PGCD}\,(5, -12) = 1$, *donc* $a' = 5$ *et* $b' = -12$. *Par le Théorème 16.12 (ii) du cours 16 [1], les solutions de* (E) *sont les couples*

$$(5 - 12k,\ 2 - 5k)\,, \quad k \in \mathbb{Z}.$$

Quand k *décrit* $\mathbb{Z}$, $-k$ *décrit aussi* $\mathbb{Z}$ *: l'ensemble des solutions de* (E) *est donc*

$$\{(5 + 12k,\ 2 + 5k) : k \in \mathbb{Z}\}\,.$$

Vérification : pour tout $k \in \mathbb{Z}$, $5\,(5 + 12k) - 12\,(2 + 5k) = 25 + 60k - 24 - 60k = 1$.

2. *Soit* $n \in \mathbb{Z}$. *Par la Définition 16.3 du cours 16 [1],* $5n \equiv 1\,[12]$ *si et seulement si* $12 \mid 5n - 1$, *c'est-à-dire s'il existe* $y \in \mathbb{Z}$ *tel que* $5n - 1 = 12y$, *ou encore tel que* (n, y) *soit une solution de* (E).

- *Si (n, y) est une solution de (E), la question 1 (c) donne $k \in \mathbb{Z}$ tel que $n = 5 + 12k$.*
- *Réciproquement, si $n = 5 + 12k$ avec $k \in \mathbb{Z}$, le couple $(n, 2 + 5k)$ est une solution de (E) (question 1 (c)).*

Donc $5n \equiv 1\,[12]$ si et seulement si $n = 5 + 12k$ avec $k \in \mathbb{Z}$, c'est-à-dire si et seulement si $12 \mid n - 5$, ou encore $n \equiv 5\,[12]$ (Définition 16.3 du cours 16 [1]). L'ensemble cherché est $\{5 + 12k : k \in \mathbb{Z}\}$.

Pour $k \leq -1$, $5 + 12k \leq -7 < 0$, et pour $k = 0$, $n = 5$: le plus petit de ces entiers qui est strictement positif est 5.

3. (a) *Par la Remarque 16.8 du cours 16 [1], il suffit de tester les nombres premiers p tels que $p^2 \leq 13$, c'est-à-dire 2 et 3 (car $5^2 = 25 > 13$). Or $13 = 2 \times 6 + 1$ et $13 = 3 \times 4 + 1$: ni 2 ni 3 ne divise 13 (Théorème 16.3 (i) du cours 16 [1]). Donc 13 est premier.*

   (b) *Soient $a \in \mathbb{Z}$ et $m \in \mathbb{N}$. On a $a^{12m+1} = \left(a^{12}\right)^m \times a$.*
   - *Si $13 \nmid a$: comme 13 est premier (question (a)), le Théorème 16.18 (i) du cours 16 [1] donne $a^{12} \equiv 1\,[13]$. Par le Théorème 16.5 (iii) puis (ii) du cours 16 [1], avec $m \in \mathbb{N}$, $a^{12m+1} \equiv 1^m \times a = a\,[13]$.*
   - *Si $13 \mid a$: alors $13 \mid a - 0$, c'est-à-dire $a \equiv 0\,[13]$ par la Définition 16.3 du cours 16, et $a^{12m+1} \equiv 0^{12m+1} = 0\,[13]$ par le Théorème 16.5 (iii) du cours 16 [1], car $12m + 1 \geq 1$. Donc $a^{12m+1} \equiv 0 \equiv a\,[13]$ (Théorème 16.4 (iii) du cours 16 [1]).*

   Dans les deux cas, $a^{12m+1} \equiv a\,[13]$.

4. *Par la question 2, $n = 5 + 12k$ avec $k \in \mathbb{Z}$. Comme $n \in \mathbb{N}$, $12k \geq -5 > -12$, donc $k > -1$, c'est-à-dire $k \geq 0$. Alors*

$$5n = 25 + 60k = 1 + 12\,(2 + 5k)\,,$$

   c'est-à-dire $5n = 12m + 1$ avec $m = 2 + 5k \in \mathbb{N}$. Par la question 3 (b), $a^{5n} = a^{12m+1} \equiv a\,[13]$ pour tout $a \in \mathbb{Z}$.

5. (a) *Soit $x \in \mathbb{Z}$ tel que $x^5 \equiv 2\,[13]$. Par le Théorème 16.5 (iii) du cours 16 [1], $\left(x^5\right)^5 \equiv 2^5\,[13]$, c'est-à-dire $x^{25} \equiv 2^5\,[13]$. Or $n = 5$ est un entier naturel tel que $5n = 25 = 1 + 12 \times 2$, donc $5n \equiv 1\,[12]$; par la question 4, $x^{25} \equiv x\,[13]$. Par le Théorème 16.4 (iii) du cours 16 [1], $x \equiv 2^5\,[13]$.*

   (b) *On a $2^5 = 32 = 13 \times 2 + 6$, donc $2^5 \equiv 6\,[13]$. Par la question (a) et le Théorème 16.4 (iii) du cours 16 [1], si $x^5 \equiv 2\,[13]$, alors $x \equiv 6\,[13]$.*

   Réciproquement, si $x \equiv 6\,[13]$, le Théorème 16.5 (iii) du cours 16 [1] donne $x^5 \equiv 6^5\,[13]$. Or $6^2 = 36 = 13 \times 2 + 10$, donc $6^2 \equiv 10\,[13]$; puis $6^4 \equiv 10^2 = 100 = 13 \times 7 + 9$, donc $6^4 \equiv 9\,[13]$; enfin $6^5 = 6^4 \times 6 \equiv 9 \times 6 = 54 = 13 \times 4 + 2$, donc $6^5 \equiv 2\,[13]$ (Théorème 16.5 (ii) et (iii) du cours 16 [1]). Ainsi $x^5 \equiv 2\,[13]$.

Les entiers cherchés sont donc les entiers $x \equiv 6\,[13]$, *c'est-à-dire l'ensemble* $\{6 + 13k : k \in \mathbb{Z}\}$.

Références

[1] Mohamed Kadhem Karray. Cours 16. Arithmétique, niveau baccalauréat. https://mohamedkadhem.com/baccalaureat/.