Exercices 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`. Comme dans le cours 16 [1], les lettres a, b, c, d, k, m, n, q, r, u, v, x, y désignent des entiers relatifs, sauf mention contraire, et la lettre p désigne toujours un nombre premier. Pour $n \in \mathbb{N}^*$, la notation $a \equiv b\,[n]$ signifie que n divise $a - b$ (Définition 16.3 du cours 16), et, pour $b \in \mathbb{N}^*$, le *reste de a par b* est le reste de la division euclidienne de a par b (Définition 16.2 du cours 16 [1]).

Table des matières

1 Divisibilité **1**

2 Division euclidienne **2**

3 Congruences **3**

4 PGCD et algorithme d'Euclide **4**

5 Bézout et Gauss **5**

6 Équation $ax + by = c$ **8**

7 Nombres premiers **10**

8 PPCM **13**

1 Divisibilité

Exercice 1 *Déterminer les entiers n tels que $n + 1$ divise $2n + 7$.*

Solution 1 *Supposons que* $n+1 \mid 2n+7$. *Comme* $n+1 \mid n+1$, *le Théorème 16.1 (iii) du cours 16 [1] donne*

$$n+1 \mid (2n+7) - 2(n+1) = 5.$$

Les diviseurs positifs de 5 *sont* 1 *et* 5 *: un tel diviseur est au plus égal à* 5 *(Théorème 16.1 (iv) du cours 16 [1]), et* 2, 3, 4 *ne divisent pas* 5, *car* $2 \times 2 < 5 < 2 \times 3$, $3 \times 1 < 5 < 3 \times 2$ *et* $4 \times 1 < 5 < 4 \times 2$. *Par l'Exemple 16.1 (iv) du cours 16 [1], les diviseurs de* 5 *sont donc* -5, -1, 1 *et* 5. *Ainsi* $n+1 \in \{-5, -1, 1, 5\}$, *c'est-à-dire* $n \in \{-6, -2, 0, 4\}$.

Réciproquement, si $n+1$ *divise* 5, *alors* $n+1$ *divise* $2(n+1)+5 = 2n+7$ *(Théorème 16.1 (iii) du cours 16 [1]). Contrôle : pour* $n = -6, -2, 0, 4$, *on a* $2n+7 = -5, 3, 7, 15$, *multiples respectifs de* $-5, -1, 1, 5$.

L'ensemble cherché est $\{-6, -2, 0, 4\}$.

Exercice 2 *Trouver tous les diviseurs positifs de* 12, *puis tous ses diviseurs dans* $\mathbb{Z}$.

Solution 2 *Soit* d *un diviseur positif de* 12. *Par le Théorème 16.1 (iv) du cours 16 [1],* $d \leq 12$. *Les égalités* $12 = 1 \times 12 = 2 \times 6 = 3 \times 4$ *montrent que* 1, 2, 3, 4, 6 *et* 12 *divisent* 12. *Il reste* 5 *et les entiers de* 7 *à* 11 *: 5 ne divise pas* 12, *car* $5 \times 2 = 10 < 12 < 15 = 5 \times 3$ *; si* $7 \leq d \leq 11$ *et* $12 = dk$ *avec* $k \in \mathbb{N}^*$, *alors* $k = 1$ *donnerait* $d = 12$, *et* $k \geq 2$ *donnerait* $dk \geq 14 > 12$, *donc* $d \nmid 12$.

Les diviseurs positifs de 12 *sont donc* $1, 2, 3, 4, 6, 12$. *Par l'Exemple 16.1 (iv) du cours 16 [1], les diviseurs de* 12 *dans* $\mathbb{Z}$ *sont ces entiers et leurs opposés :*

$$\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12.$$

2 Division euclidienne

Exercice 3

1. *Effectuer la division euclidienne de* 123 *par* 11.
2. *Effectuer la division euclidienne de* 1001 *par* 14. *L'entier* 14 *divise-t-il* 1001 *?*
3. *Effectuer la division euclidienne de* -1001 *par* 14.

Solution 3 *Les entiers* 11 *et* 14 *sont dans* $\mathbb{N}^*$ *: le Théorème 16.2 du cours 16 [1] s'applique, et le couple* (q, r) *tel que* $a = bq + r$ *et* $0 \leq r < b$ *est unique. Il suffit donc d'en trouver un.*

1. $123 = 11 \times 11 + 2$ *et* $0 \leq 2 < 11$ *: le quotient est* 11 *et le reste est* 2 *(Définition 16.2 du cours 16 [1]).*
2. $1001 = 14 \times 71 + 7$ *et* $0 \leq 7 < 14$ *: le quotient est* 71 *et le reste est* 7. *Ce reste n'est pas nul, donc* 14 *ne divise pas* 1001 *(Théorème 16.3 (i) du cours 16 [1]).*
3. *De* $1001 = 14 \times 71 + 7$, *on tire* $-1001 = 14 \times (-71) - 7 = 14 \times (-72) + 7$, *et* $0 \leq 7 < 14$. *Le quotient est* -72 *et le reste est* 7 *(et non* -7*), comme dans l'Exemple 16.2 (ii) du cours 16 [1].*

3 Congruences

Exercice 4 *Sans calculer ces nombres, déterminer le reste par* 9 *de* $1234+5678$, *de* 1234×5678 *et de* 5678^3.

Solution 4 *On a* $1234 = 9 \times 137 + 1$ *et* $5678 = 9 \times 630 + 8$, *donc* $1234 \equiv 1\,[9]$ *et* $5678 \equiv 8\,[9]$ *(Définition 16.3 du cours 16 [1]).*

- *Par le Théorème 16.5 (i) du cours 16 [1],* $1234+5678 \equiv 1+8 = 9 \equiv 0\,[9]$. *Le reste est* 0 *(Théorème 16.4 (ii) et (iii) du cours 16 [1]) :* $1234+5678$ *est divisible par* 9.
- *Par le Théorème 16.5 (ii) du cours 16 [1],* $1234 \times 5678 \equiv 1 \times 8 = 8\,[9]$. *Comme* $0 \leq 8 < 9$, *le reste est* 8 *(Théorème 16.4 (ii) du cours 16 [1]).*
- *On a* $8 \equiv -1\,[9]$, *car* $8-(-1) = 9$, *donc* $5678 \equiv -1\,[9]$ *(Théorème 16.4 (iii) du cours 16 [1]). Par le Théorème 16.5 (iii) du cours 16 [1],* $5678^3 \equiv (-1)^3 = -1 \equiv 8\,[9]$. *Le reste est* 8 *(Théorème 16.4 (ii) du cours 16 [1]).*

Exercice 5

1. *Montrer que, pour tout* $n \in \mathbb{Z}$, *le reste de* n^2 *par* 4 *est* 0 *ou* 1.
2. *En déduire que* 2027 *n'est pas la somme des carrés de deux entiers.*

Solution 5

1. *Par le Théorème 16.3 (ii) du cours 16 [1],* n *s'écrit* $4q+r$ *avec* $q \in \mathbb{Z}$ *et* $r \in \{0,1,2,3\}$ *; alors* $n-r = 4q$, *donc* $n \equiv r\,[4]$. *Par le Théorème 16.5 (iii) du cours 16 [1],* $n^2 \equiv r^2\,[4]$, *avec* $r^2 \in \{0,1,4,9\}$. *Or* $4 \equiv 0\,[4]$ *et* $9 = 4 \times 2 + 1 \equiv 1\,[4]$. *Donc* $n^2 \equiv 0\,[4]$ *ou* $n^2 \equiv 1\,[4]$ *(Théorème 16.4 (iii) du cours 16), et le reste de* n^2 *par* 4 *est* 0 *ou* 1 *(Théorème 16.4 (ii) du cours 16 [1]).*
2. *Soient* $a, b \in \mathbb{Z}$. *Par la question 1,* $a^2 \equiv r_1\,[4]$ *et* $b^2 \equiv r_2\,[4]$ *avec* $r_1, r_2 \in \{0,1\}$, *donc* $a^2+b^2 \equiv r_1+r_2\,[4]$ *(Théorème 16.5 (i) du cours 16 [1]), avec* $r_1+r_2 \in \{0,1,2\}$. *Le reste de* a^2+b^2 *par* 4 *est donc* 0, 1 *ou* 2 *(Théorème 16.4 (ii) du cours 16 [1]). Or* $2027 = 4 \times 506 + 3$ *: le reste de* 2027 *par* 4 *est* 3. *Deux entiers égaux ont le même reste, donc* $a^2+b^2 \neq 2027$, *et cela pour tous* $a, b \in \mathbb{Z}$.

Exercice 6

1. *Trouver le reste de* 2^5 *par* 7.
2. *Trouver le reste de* 2^{10} *par* 17.

Solution 6

1. $2^3 = 8 = 7+1$, *donc* $2^3 \equiv 1\,[7]$. *Par le Théorème 16.5 (ii) du cours 16 [1],*

$$2^5 = 2^3 \times 2^2 \equiv 1 \times 4 = 4\,[7]\,.$$

Comme $0 \leq 4 < 7$, *le reste de* 2^5 *par* 7 *est* 4 *(Théorème 16.4 (ii) du cours 16 [1]). Contrôle :* $2^5 = 32 = 7 \times 4 + 4$.

2. $2^4 = 16$ *et* $16 - (-1) = 17$, *donc* $2^4 \equiv -1\,[17]$. *Par le Théorème 16.5 (iii) du cours 16,* $2^8 = \left(2^4\right)^2 \equiv (-1)^2 = 1\,[17]$, *puis, par le Théorème 16.5 (ii) du cours 16 [1],*

$$2^{10} = 2^8 \times 2^2 \equiv 1 \times 4 = 4\,[17]\,.$$

Comme $0 \leq 4 < 17$, *le reste de* 2^{10} *par* 17 *est* 4 *(Théorème 16.4 (ii) du cours 16 [1]). Contrôle :* $2^{10} = 1024 = 17 \times 60 + 4$.

4 PGCD et algorithme d'Euclide

Exercice 7 *Calculer* $\mathrm{PGCD}\,(18, 15)$.

Solution 7 *On applique l'algorithme d'Euclide (Théorème 16.7 du cours 16 [1]) à* 18 *et* 15, *qui sont dans* $\mathbb{N}^*$ *:*

$$18 = 15 \times 1 + 3,$$
$$15 = 3 \times 5 + 0.$$

Le dernier reste non nul est 3, *donc* $\mathrm{PGCD}\,(18, 15) = 3$ *(Théorème 16.7 (iii) du cours 16 [1]). On peut aussi utiliser les décompositions* $18 = 2 \times 3^2$ *et* $15 = 3 \times 5$ *: le seul nombre premier commun est* 3, *avec les exposants* 2 *et* 1, *et le Théorème 16.17 du cours 16 [1] donne le même résultat,* $3^1 = 3$.

Exercice 8 *Soit* $n \in \mathbb{Z}$.

1. *Montrer que* n *et* $n + 1$ *sont premiers entre eux.*
2. *Montrer que* $\mathrm{PGCD}\,(n + 5, n + 2)$ *vaut* 3 *si* $n \equiv 1\,[3]$, *et* 1 *sinon.*

Solution 8

1. *Les entiers* n *et* $n+1$ *ne sont pas tous deux nuls. Comme* $n+1 = n \times 1+1$, *le Théorème 16.6 du cours 16 [1] dit que les diviseurs communs de* $n + 1$ *et* n *sont les diviseurs communs de* n *et* 1. *Ce sont les diviseurs de* 1, *qui divisent aussi* n *(Théorème 16.1 (ii) du cours 16), c'est-à-dire* 1 *et* -1, *car* 0 *ne divise pas* 1 *(Théorème 16.1 (iv) et Exemple 16.1 (ii) du cours 16 [1]). Le plus grand est* 1, *donc* $\mathrm{PGCD}\,(n, n + 1) = 1$ *(Remarque 16.4 (i) du cours 16) :* n *et* $n+1$ *sont premiers entre eux (Définition 16.5 du cours 16 [1]).*

2. *Les entiers* $n + 5$ *et* $n + 2$ *diffèrent de* 3, *donc ne sont pas tous deux nuls. Comme* $n + 5 = (n + 2) \times 1 + 3$, *le Théorème 16.6 du cours 16 [1] dit que* $n + 5$ *et* $n + 2$ *ont les mêmes diviseurs communs que* $n + 2$ *et* 3. *Ces deux ensembles sont égaux, donc ont le même plus grand élément (Définition 16.4 du cours 16 [1]) :*

$$\mathrm{PGCD}\,(n + 5, n + 2) = \mathrm{PGCD}\,(3, n + 2)\,.$$

Ce PGCD est un diviseur positif de 3, *donc vaut* 1 *ou* 3, *car* $2 \nmid 3$ *(Théorème 16.1 (iv) du cours 16 [1]).*

- *Si* $3 \mid n+2$, *alors* $\mathrm{PGCD}\,(3, n+2) = 3$ *(Remarque 16.4 (ii) du cours 16 [1]).*
- *Si* $3 \nmid n+2$, *alors* $\mathrm{PGCD}\,(3, n+2) \neq 3$, *car ce PGCD divise* $n+2$ *; il vaut donc* 1.

Enfin, $n+2 = (n-1)+3$, *donc* $3 \mid n+2$ *si et seulement si* $3 \mid n-1$ *(Théorème 16.1 (iii) du cours 16, dans les deux sens), c'est-à-dire si et seulement si* $n \equiv 1\,[3]$ *(Définition 16.3 du cours 16 [1]). Par exemple,* $\mathrm{PGCD}\,(6,3) = 3$ *pour* $n = 1$, *et* $\mathrm{PGCD}\,(5,2) = 1$ *pour* $n = 0$.

Exercice 9 *Calculer* $\mathrm{PGCD}\,(48, 180)$ *par l'algorithme d'Euclide.*

Solution 9 *L'algorithme d'Euclide (Théorème 16.7 et Remarque 16.4 (i) du cours 16 [1]) procède par divisions euclidiennes successives : on divise* 180 *par* 48, *puis* 48 *par le reste obtenu, et ainsi de suite, jusqu'à un reste nul.*

$$\begin{aligned} 180 &= 48 \times 3 + 36, \\ 48 &= 36 \times 1 + 12, \\ 36 &= 12 \times 3 + 0. \end{aligned}$$

Le dernier reste non nul est 12, *donc* $\mathrm{PGCD}\,(48, 180) = 12$ *(Théorème 16.7 (iii) du cours 16 [1]).*

5 Bézout et Gauss

Exercice 10 *On a montré à l'exercice 9 que* $\mathrm{PGCD}\,(48, 180) = 12$. *En remontant les divisions de cet exercice, trouver* $u, v \in \mathbb{Z}$ *tels que*

$$48u + 180v = 12.$$

Solution 10 *Un tel couple existe par le Théorème 16.9 du cours 16 [1]. 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, avec les divisions de l'exercice 9 :*

$$\begin{aligned} 12 &= 48 - 36 \times 1 \\ &= 48 - (180 - 48 \times 3) \\ &= 48 \times 4 - 180. \end{aligned}$$

On peut donc prendre $u = 4$ *et* $v = -1$. *Contrôle :* $48 \times 4 - 180 = 192 - 180 = 12$. *Ce couple n'est pas le seul : par la Remarque 16.6 du cours 16 [1],* $(4 + 180, -1 - 48) = (184, -49)$ *convient aussi.*

Exercice 11 *Calculer* $\mathrm{PGCD}\,(56, 81)$ *par l'algorithme d'Euclide, puis l'écrire sous la forme* $56u + 81v$, *avec* $u, v \in \mathbb{Z}$, *en remontant les divisions.*

Solution 11 *Par l'algorithme d'Euclide (Théorème 16.7 et Remarque 16.4 (i) du cours 16 [1]), appliqué à* 81 *et* 56 *:*

$$\begin{aligned} 81 &= 56 \times 1 + 25, \\ 56 &= 25 \times 2 + 6, \\ 25 &= 6 \times 4 + 1, \\ 6 &= 1 \times 6 + 0. \end{aligned}$$

Le dernier reste non nul est 1*, donc* $\mathrm{PGCD}\,(56, 81) = 1$ *: 56 et 81 sont premiers entre eux. On remonte ensuite les divisions (Exemple 16.7 du cours 16 [1]) :*

$$\begin{aligned} 1 &= 25 - 6 \times 4 \\ &= 25 - (56 - 25 \times 2) \times 4 = 25 \times 9 - 56 \times 4 \\ &= (81 - 56) \times 9 - 56 \times 4 = 81 \times 9 - 56 \times 13. \end{aligned}$$

Donc $1 = 56 \times (-13) + 81 \times 9$*, soit* $u = -13$ *et* $v = 9$*. Contrôle :* $81 \times 9 - 56 \times 13 = 729 - 728 = 1$*.*

Exercice 12

1. *Montrer que* 11 *et* 26 *sont premiers entre eux et trouver* $u, v \in \mathbb{Z}$ *tels que* $11u + 26v = 1$*.*
2. *En déduire un inverse de* 11 *modulo* 26 *compris entre* 0 *et* 25*.*
3. *Résoudre dans* $\mathbb{Z}$ *la congruence* $11x \equiv 5\,[26]$*.*

Solution 12

1. *Par l'algorithme d'Euclide (Théorème 16.7 et Remarque 16.4 (i) du cours 16 [1]) :*

$$\begin{aligned} 26 &= 11 \times 2 + 4, \\ 11 &= 4 \times 2 + 3, \\ 4 &= 3 \times 1 + 1, \\ 3 &= 1 \times 3 + 0. \end{aligned}$$

   Le dernier reste non nul est 1*, donc* $\mathrm{PGCD}\,(11, 26) = 1$*. En remontant les divisions (Exemple 16.7 du cours 16 [1]) :*

$$\begin{aligned} 1 &= 4 - 3 = 4 - (11 - 2 \times 4) = 3 \times 4 - 11 \\ &= 3 \times (26 - 2 \times 11) - 11 = 3 \times 26 - 7 \times 11. \end{aligned}$$

   Donc $11 \times (-7) + 26 \times 3 = 1$ *: u* $= -7$ *et v* $= 3$*. Contrôle :* $78 - 77 = 1$*.*

2. *De* $11 \times (-7) = 1 - 3 \times 26$*, on tire* $11 \times (-7) \equiv 1\,[26]$ *: −7 est un inverse de* 11 *modulo* 26 *(Corollaire 16.3 du cours 16 [1], avec* $26 \geq 2$*). Comme* $19 - (-7) = 26$*, on a* $19 \equiv -7\,[26]$*, donc* $11 \times 19 \equiv 11 \times (-7) \equiv 1\,[26]$ *(Théorème 16.5 (ii) et Théorème 16.4 (iii) du cours 16 [1]). L'inverse cherché est* 19*. Contrôle :* $11 \times 19 = 209 = 8 \times 26 + 1$*.*

3. *Si* $11x \equiv 5\,[26]$*, on multiplie par* 19 *(Théorème 16.5 (ii) du cours 16 [1]) :* $209x \equiv 95\,[26]$*. Or* $209 \equiv 1\,[26]$ *et* $95 = 3 \times 26 + 17 \equiv 17\,[26]$*, donc* $x \equiv 17\,[26]$ *(Théorème 16.5 (ii) et Théorème 16.4 (iii) du cours 16 [1]). Réciproquement, si* $x \equiv 17\,[26]$*, alors* $11x \equiv 11 \times 17 = 187\,[26]$ *(Théorème 16.5 (ii) du cours 16 [1]), et* $187 = 7 \times 26 + 5 \equiv 5\,[26]$*. Les solutions sont les entiers* $17 + 26k$*,* $k \in \mathbb{Z}$ *:*

$$\{x \in \mathbb{Z} : 11x \equiv 5\,[26]\} = \{17 + 26k : k \in \mathbb{Z}\}\,.$$

Exercice 13 *Déterminer les couples* $(x, y) \in \mathbb{Z}^2$ *tels que* $7x = 12y$*.*

Solution 13 *Par l'algorithme d'Euclide (Théorème 16.7 et Remarque 16.4 (i) du cours 16 [1]),* $12 = 7 \times 1 + 5$*,* $7 = 5 \times 1 + 2$*,* $5 = 2 \times 2 + 1$*,* $2 = 1 \times 2 + 0$ *:* $\mathrm{PGCD}\,(7, 12) = 1$*, donc* 7 *et* 12 *sont premiers entre eux.*

Soit (x, y) *un couple tel que* $7x = 12y$*. Alors* $7 \mid 12y$*, et* 7 *est premier avec* 12*, donc* $7 \mid y$ *par le théorème de Gauss (Théorème 16.11 du cours 16 [1]). Écrivons* $y = 7k$ *avec* $k \in \mathbb{Z}$ *: alors* $7x = 84k$*, donc* $x = 12k$*.*

Réciproquement, pour tout $k \in \mathbb{Z}$*, le couple* $(12k, 7k)$ *convient, car* $7 \times 12k = 84k = 12 \times 7k$*. L'ensemble des solutions est*

$$\{(12k, 7k) : k \in \mathbb{Z}\}\,.$$

Exercice 14 *Montrer que, pour tout* $n \in \mathbb{Z}$*, l'entier* $n\,(n+1)\,(n+2)$ *est divisible par* 6*.*

Solution 14 *Notons* $P = n\,(n+1)\,(n+2)$*.*

- *Par le Théorème 16.3 (ii) du cours 16 [1],* n *s'écrit* $3q$*,* $3q{+}1$ *ou* $3q{+}2$*, avec* $q \in \mathbb{Z}$*. Dans le premier cas,* $3 \mid n$ *; dans le deuxième,* $n + 2 = 3\,(q+1)$ *; dans le troisième,* $n + 1 = 3\,(q+1)$*. Ainsi* 3 *divise l'un des trois facteurs de* P*, donc divise* P *(Théorème 16.1 (i) du cours 16 [1]).*

- *De même,* n *s'écrit* $2q$ *ou* $2q + 1$ *:* 2 *divise* n *ou* $n + 1 = 2\,(q+1)$*, donc* $2 \mid P$*.*

Les entiers 2 *et* 3 *sont premiers entre eux :* $3 = 2 \times 1 + 1$ *et* $2 = 1 \times 2 + 0$*, donc* $\mathrm{PGCD}\,(2, 3) = 1$ *(Théorème 16.7 et Remarque 16.4 (i) du cours 16 [1]). Comme* $2 \mid P$ *et* $3 \mid P$*, le Corollaire 16.4 du cours 16 [1] donne* $6 \mid P$*.*

Exercice 15 *Soient* $a, b, c \in \mathbb{Z}$*. On suppose que* a *et* b *sont premiers entre eux, et que* a *et* c *sont premiers entre eux.*

1. *Montrer que* a *et* bc *sont premiers entre eux.*

2. *En déduire, avec l'exercice 8, que pour tout* $n \in \mathbb{Z}$*, les entiers* n *et* $n^2 - 1$ *sont premiers entre eux.*

Solution 15

1. *Par le théorème de Bézout (Théorème 16.10 du cours 16 [1]), il existe* $u, v, u', v' \in \mathbb{Z}$ *tels que* $au + bv = 1$ *et* $au' + cv' = 1$. *En multipliant ces deux égalités,*

$$1 = (au + bv)(au' + cv') = a(auu' + ucv' + bvu') + bc(vv').$$

Les entiers a *et* bc *ne sont pas tous deux nuls, sinon le membre de droite serait nul. L'égalité ci-dessus est de la forme* $aU + (bc)V = 1$ *avec* $U, V \in \mathbb{Z}$, *donc* a *et* bc *sont premiers entre eux, par le Théorème 16.10 du cours 16 [1].*

2. *Soit* $n \in \mathbb{Z}$. *Par l'exercice 8 (question 1),* n *et* $n+1$ *sont premiers entre eux ; appliquée à l'entier* $n-1$, *la même question montre que* $n-1$ *et* n *sont premiers entre eux, donc* n *et* $n-1$ *aussi (Remarque 16.4 (i) du cours 16 [1]). La question 1, avec* $a = n$, $b = n-1$ *et* $c = n+1$, *montre que* n *et* $(n-1)(n+1) = n^2 - 1$ *sont premiers entre eux.*

6 Équation $ax + by = c$

Exercice 16 1. *Calculer* $\mathrm{PGCD}(91, 35)$.

2. *L'équation* $91x + 35y = 5$ *a-t-elle des solutions* $(x, y) \in \mathbb{Z}^2$ *?*

3. *Résoudre dans* $\mathbb{Z}^2$ *l'équation* $91x + 35y = 7$.

Solution 16

1. *Par l'algorithme d'Euclide (Théorème 16.7 du cours 16 [1]) :*

$$\begin{aligned} 91 &= 35 \times 2 + 21, \\ 35 &= 21 \times 1 + 14, \\ 21 &= 14 \times 1 + 7, \\ 14 &= 7 \times 2 + 0. \end{aligned}$$

Le dernier reste non nul est 7, *donc* $\mathrm{PGCD}(91, 35) = 7$.

2. *Les entiers* 91 *et* 35 *sont non nuls, et* $7 \nmid 5$. *Par le Théorème 16.12 (i) du cours 16 [1], l'équation* $91x + 35y = 5$ *n'a pas de solution : l'ensemble de ses solutions est vide.*

3. *On suit la méthode de l'Exemple 16.8 du cours 16 [1].*

Étape 1 (existence). $\mathrm{PGCD}(91, 35) = 7$ *et* $7 \mid 7$ *: il y a des solutions (Théorème 16.12 (i) du cours 16 [1]).*

Étape 2 (solution particulière). *On remonte les divisions de la question 1 (Exemple 16.7 du cours 16 [1]) :*

$$\begin{aligned} 7 &= 21 - 14 = 21 - (35 - 21) = 2 \times 21 - 35 \\ &= 2 \times (91 - 2 \times 35) - 35 = 2 \times 91 - 5 \times 35. \end{aligned}$$

Donc $(x_0, y_0) = (2, -5)$ *est une solution :* $182 - 175 = 7$.

Étape 3 (toutes les solutions). *Ici* $91 = 7 \times 13$ *et* $35 = 7 \times 5$, *donc* $a' = 13$ *et* $b' = 5$. *Par le Théorème 16.12 (ii) du cours 16 [1], les solutions sont les couples* $(2 + 5k,\ -5 - 13k)$, $k \in \mathbb{Z}$:

$$\left\{(x, y) \in \mathbb{Z}^2 : 91x + 35y = 7\right\} = \left\{(2 + 5k,\ -5 - 13k) : k \in \mathbb{Z}\right\}.$$

Vérification. *Pour* $k = 1$: $(7, -18)$, *et* $91 \times 7 + 35 \times (-18) = 637 - 630 = 7$.

Exercice 17 *1. Résoudre dans* $\mathbb{Z}^2$ *l'équation* $23x + 17y = 4$.

2. Déterminer l'unique solution (x, y) *telle que* $0 \leq y < 23$.

Solution 17

1. *On suit la méthode de l'Exemple 16.8 du cours 16 [1]. Les entiers* 23 *et* 17 *sont non nuls.*

   Étape 1 (existence). *Par l'algorithme d'Euclide (Théorème 16.7 du cours 16 [1]) :*

   $$\begin{aligned} 23 &= 17 \times 1 + 6, \\ 17 &= 6 \times 2 + 5, \\ 6 &= 5 \times 1 + 1, \\ 5 &= 1 \times 5 + 0. \end{aligned}$$

   Donc $\mathrm{PGCD}\,(23, 17) = 1$, *et* $1 \mid 4$: *il y a des solutions (Théorème 16.12 (i) du cours 16 [1]).*

   Étape 2 (solution particulière). *On remonte les divisions (Exemple 16.7 du cours 16 [1]) :*

   $$\begin{aligned} 1 &= 6 - 5 = 6 - (17 - 2 \times 6) = 3 \times 6 - 17 \\ &= 3 \times (23 - 17) - 17 = 3 \times 23 - 4 \times 17. \end{aligned}$$

   En multipliant par 4 : $23 \times 12 + 17 \times (-16) = 4$, *donc* $(x_0, y_0) = (12, -16)$ *est une solution (*$276 - 272 = 4$*).*

   Étape 3 (toutes les solutions). *Ici* $d = 1$, *donc* $a' = 23$ *et* $b' = 17$. *Par le Théorème 16.12 (ii) du cours 16 [1], les solutions sont les couples* $(12 + 17k,\ -16 - 23k)$, $k \in \mathbb{Z}$.

   Vérification. *Pour* $k = -1$: $(-5, 7)$, *et* $23 \times (-5) + 17 \times 7 = -115 + 119 = 4$.

2. *Par la question 1, une solution s'écrit* $(12 + 17k,\ -16 - 23k)$ *avec* $k \in \mathbb{Z}$. *La condition* $0 \leq -16 - 23k < 23$ *équivaut à* $-39 < 23k \leq -16$. *Pour* $k \geq 0$, *on a* $23k \geq 0 > -16$ *; pour* $k \leq -2$, *on a* $23k \leq -46 < -39$ *; pour* $k = -1$, *on a* $23k = -23$, *qui convient. Le seul entier qui convient est donc* $k = -1$, *et la solution cherchée est* $(-5, 7)$.

Exercice 18 *On cherche les entiers n tels que $n \equiv 2\,[5]$ et $n \equiv 3\,[7]$.*

1. *Soit n un tel entier. Montrer qu'il existe $(x, y) \in \mathbb{Z}^2$ tel que $n = 2 + 5x = 3 + 7y$, et que $5x - 7y = 1$.*
2. *Résoudre dans $\mathbb{Z}^2$ l'équation $5x - 7y = 1$.*
3. *En déduire que $n \equiv 2\,[5]$ et $n \equiv 3\,[7]$ si et seulement si $n \equiv 17\,[35]$. Donner les solutions comprises entre 0 et 100.*

Solution 18

1. *Par la Définition 16.3 du cours 16 [1], $5 \mid n - 2$ et $7 \mid n - 3$: il existe $x, y \in \mathbb{Z}$ tels que $n - 2 = 5x$ et $n - 3 = 7y$. Alors $n = 2 + 5x = 3 + 7y$, d'où $5x - 7y = 1$.*
2. *On suit la méthode de l'Exemple 16.8 du cours 16 [1], avec $a = 5$ et $b = -7$, non nuls.*

   Étape 1 (existence). $\mathrm{PGCD}\,(5, -7) = \mathrm{PGCD}\,(5, 7)$ *(Remarque 16.4 (i) du cours 16), et l'algorithme d'Euclide donne $7 = 5 \times 1 + 2$, $5 = 2 \times 2 + 1$, $2 = 1 \times 2 + 0$, donc ce PGCD vaut 1 (Théorème 16.7 et Remarque 16.4 (i) du cours 16 [1]). Comme $1 \mid 1$, il y a des solutions (Théorème 16.12 (i) du cours 16 [1]).*

   Étape 2 (solution particulière). $5 \times 3 - 7 \times 2 = 15 - 14 = 1$ *: $(x_0, y_0) = (3, 2)$.*

   Étape 3 (toutes les solutions). *Ici $d = 1$, $a' = 5$ et $b' = -7$. Par le Théorème 16.12 (ii) du cours 16 [1], les solutions sont les couples $(3 - 7k,\ 2 - 5k)$, $k \in \mathbb{Z}$.*

   Vérification. *Pour $k = 1$: $(-4, -3)$, et $5 \times (-4) - 7 \times (-3) = -20 + 21 = 1$.*
3. *Si $n \equiv 2\,[5]$ et $n \equiv 3\,[7]$, les questions 1 et 2 donnent $k \in \mathbb{Z}$ tel que $x = 3 - 7k$, donc $n = 2 + 5\,(3 - 7k) = 17 - 35k$, et $n \equiv 17\,[35]$.*

   Réciproquement, si $n = 17 + 35m$ avec $m \in \mathbb{Z}$, alors $n - 2 = 5\,(3 + 7m)$ et $n - 3 = 7\,(2 + 5m)$, donc $n \equiv 2\,[5]$ et $n \equiv 3\,[7]$. L'ensemble cherché est

   $$\{17 + 35m : m \in \mathbb{Z}\}\,.$$

   Entre 0 et 100, on trouve 17, 52 et 87 ($m = 0, 1, 2$) ; pour $m = -1$ et $m = 3$, on obtient -18 et 122.

7 Nombres premiers

Exercice 19 1. *L'entier 29 est-il premier ?*

2. *Trouver tous les nombres premiers inférieurs à 20.*

Solution 19 *On utilise le test de primalité suivant (Remarque 16.8 du cours 16 [1]) : un entier $n \geq 2$ est premier si et seulement si aucun nombre premier p tel que $p^2 \leq n$ ne divise n.*

1. *Les nombres premiers p tels que $p^2 \leq 29$ sont 2, 3 et 5, car $7^2 = 49 > 29$. Or $29 = 2 \times 14 + 1 = 3 \times 9 + 2 = 5 \times 5 + 4$: les restes ne sont pas nuls, donc 2, 3 et 5 ne divisent pas 29 (Théorème 16.3 (i) du cours 16 [1]). Ainsi 29 est premier.*

2. *Les entiers 2 et 3 sont premiers : aucun nombre premier p ne vérifie $p^2 \leq 3$, car $2^2 = 4 > 3$. Pour $4 \leq n \leq 19$, les nombres premiers p tels que $p^2 \leq n$ sont parmi 2 et 3, car 4 n'est pas premier ($2 \mid 4$) et $5^2 = 25 > 19$. Les entiers de 4 à 19 qui ne sont divisibles ni par 2 ni par 3 sont 5, 7, 11, 13, 17 et 19 : ils sont premiers. Les autres sont divisibles par 2 ou par 3 et différents de 2 et de 3, donc ont au moins trois diviseurs positifs (1, 2 ou 3, et eux-mêmes) : ils ne sont pas premiers (Définition 16.6 du cours 16 [1]). Enfin, 0 et 1 ne sont pas premiers (Exemple 16.9 du cours 16 [1]). Les nombres premiers inférieurs à 20 sont donc*

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19.$$

Exercice 20 1. *Décomposer 2520 en facteurs premiers.*

2. *Combien 2520 a-t-il de diviseurs positifs ?*

3. *Décomposer 1188 en facteurs premiers, et en déduire* $\mathrm{PGCD}(2520, 1188)$.

Solution 20

1. *Comme dans la Remarque 16.9 du cours 16 [1], on divise par le plus petit diviseur premier, puis le quotient par le sien, et ainsi de suite. On a $2520 = 2 \times 1260$, $1260 = 2 \times 630$, $630 = 2 \times 315$; 315 est impair et $315 = 3 \times 105$, $105 = 3 \times 35$; 35 n'est pas divisible par 3 ($35 = 3 \times 11 + 2$) et $35 = 5 \times 7$, où 7 est premier. Donc*

$$2520 = 2^3 \times 3^2 \times 5 \times 7,$$

et c'est la décomposition de 2520 (Théorème 16.16 du cours 16 [1]).

2. *Par le Théorème 16.17 du cours 16 [1], les diviseurs positifs de 2520 sont les entiers $2^{e_1}3^{e_2}5^{e_3}7^{e_4}$ avec $0 \leq e_1 \leq 3$, $0 \leq e_2 \leq 2$, $0 \leq e_3 \leq 1$ et $0 \leq e_4 \leq 1$. Ils sont deux à deux distincts (Théorème 16.17 du cours 16 [1]), donc 2520 a $(3+1)(2+1)(1+1)(1+1) = 48$ diviseurs positifs.*

3. *De même, $1188 = 2 \times 594$, $594 = 2 \times 297$, $297 = 3 \times 99$, $99 = 3 \times 33$, $33 = 3 \times 11$, où 11 est premier : $1188 = 2^2 \times 3^3 \times 11$. Les nombres premiers communs aux deux décompositions sont 2 et 3 ; les plus petits exposants sont $\min(3,2) = 2$ et $\min(2,3) = 2$. Par le Théorème 16.17 du cours 16 [1],*

$$\mathrm{PGCD}(2520, 1188) = 2^2 \times 3^2 = 36.$$

Contrôle : $2520 = 36 \times 70$ et $1188 = 36 \times 33$.

Exercice 21 *Soit p un nombre premier.*

1. *Soit $n \in \mathbb{Z}$. Montrer que si p divise n^2, alors p^2 divise n^2.*

2. *En déduire que 12 n'est le carré d'aucun entier.*

Solution 21

1. *Si $p \mid n^2 = n \times n$, le Théorème 16.15 (ii) du cours 16 [1] donne $p \mid n$. Écrivons $n = pk$ avec $k \in \mathbb{Z}$: alors $n^2 = p^2k^2$, donc $p^2 \mid n^2$.*

2. *Le nombre 3 est premier : ses diviseurs positifs sont au plus égaux à 3 (Théorème 16.1 (iv) du cours 16 [1]), et $2 \nmid 3$. Soit $n \in \mathbb{Z}$. Si l'on avait $n^2 = 12$, alors 3 diviserait n^2, puisque $12 = 3 \times 4$, donc 9 diviserait 12 par la question 1. Or $12 = 9 \times 1 + 3$, et ce reste n'est pas nul, donc $9 \nmid 12$ (Théorème 16.3 (i) du cours 16 [1]). Ainsi $n^2 \neq 12$ pour tout $n \in \mathbb{Z}$.*

Exercice 22 *Trouver tous les entiers n tels que $\mathrm{PGCD}(n, 18) = 2$ et $\mathrm{PGCD}(n, 35) = 5$.*

Solution 22 *On a $18 = 2 \times 3^2$ et $35 = 5 \times 7$. Par le Théorème 16.17 du cours 16 [1], les diviseurs positifs de 18 sont $1, 2, 3, 6, 9, 18$, et ceux de 35 sont $1, 5, 7, 35$.*

Étape 1. *Montrons que $\mathrm{PGCD}(n, 18) = 2$ si et seulement si $2 \mid n$ et $3 \nmid n$. Notons $d = \mathrm{PGCD}(n, 18)$, qui est un diviseur positif de 18.*

- *Si $d = 2$, alors $2 \mid n$. Si l'on avait $3 \mid n$, alors 3, qui divise aussi 18, diviserait $d = 2$ (Corollaire 16.1 du cours 16 [1]) : c'est faux. Donc $3 \nmid n$.*

- *Si $2 \mid n$ et $3 \nmid n$, alors 2 divise n et 18, donc $2 \mid d$ (Corollaire 16.1 du cours 16 [1]). De plus $3 \nmid d$, car $3 \mid d$ et $d \mid n$ donneraient $3 \mid n$ (Théorème 16.1 (ii) du cours 16 [1]). Parmi les entiers 1, 2, 3, 6, 9 et 18, le seul qui soit pair et non divisible par 3 est 2 : donc $d = 2$.*

Étape 2. *Le même raisonnement, où 2, 3 et 18 sont remplacés par 5, 7 et 35, montre que $\mathrm{PGCD}(n, 35) = 5$ si et seulement si $5 \mid n$ et $7 \nmid n$. Il utilise le fait que, parmi les diviseurs positifs 1, 5, 7 et 35 de 35, le seul multiple de 5 non divisible par 7 est 5.*

Étape 3. *Les entiers 2 et 5 sont premiers entre eux ($5 = 2 \times 2 + 1$, $2 = 1 \times 2 + 0$), par l'algorithme d'Euclide (Théorème 16.7 et Remarque 16.4 (i) du cours 16 [1]). Si $2 \mid n$ et $5 \mid n$, alors $10 \mid n$ (Corollaire 16.4 du cours 16) ; réciproquement, si $10 \mid n$, alors $2 \mid n$ et $5 \mid n$ (Théorème 16.1 (ii) du cours 16 [1]). Les entiers cherchés sont donc les $n = 10k$, $k \in \mathbb{Z}$, tels que $3 \nmid 10k$ et $7 \nmid 10k$.*

Étape 4. *Les entiers 3 et 10 sont premiers entre eux ($10 = 3 \times 3 + 1$, $3 = 1 \times 3 + 0$), de même que 7 et 10 ($10 = 7 \times 1 + 3$, $7 = 3 \times 2 + 1$, $3 = 1 \times 3 + 0$), par l'algorithme d'Euclide (Théorème 16.7 et Remarque 16.4 (i) du cours 16 [1]). Si $3 \mid 10k$, alors $3 \mid k$ par le théorème de Gauss (Théorème 16.11 du cours 16) ;*

réciproquement, si $3 \mid k$*, alors* $3 \mid 10k$ *(Théorème 16.1 (i) du cours 16 [1]). Donc* $3 \mid 10k$ *si et seulement si* $3 \mid k$*, et de même* $7 \mid 10k$ *si et seulement si* $7 \mid k$*.*

Chaque étape est une équivalence. L'ensemble cherché est donc

$$\{10k : k \in \mathbb{Z},\ 3 \nmid k \text{ et } 7 \nmid k\}.$$

Par exemple, $n = 10$ *convient :* $\mathrm{PGCD}(10, 18) = 2$ *et* $\mathrm{PGCD}(10, 35) = 5$*. En revanche,* $n = 0$ *ne convient pas, car* $\mathrm{PGCD}(0, 18) = 18$*.*

Exercice 23 *1. Montrer que* 11 *est premier, puis déterminer le reste de* 2^{2026} *par* 11*.*

2. En déduire que $2^{2026} + 2$ *est divisible par* 11*.*

Solution 23

1. Les nombres premiers p *tels que* $p^2 \leq 11$ *sont* 2 *et* 3*, car* $5^2 = 25 > 11$ *; or* $11 = 2 \times 5 + 1 = 3 \times 3 + 2$*, donc ni* 2 *ni* 3 *ne divise* 11 *(Théorème 16.3 (i) du cours 16), et* 11 *est premier (Remarque 16.8 du cours 16 [1]).*

Comme 11 *est premier et* $11 \nmid 2$ *(*$0 < 2 < 11$*), le petit théorème de Fermat (Théorème 16.18 (i) du cours 16 [1]) donne* $2^{10} \equiv 1\,[11]$*. On divise l'exposant par* 10 *:* $2026 = 10 \times 202 + 6$*, donc, par le Théorème 16.5 (iii) puis (ii) du cours 16 [1],*

$$2^{2026} = \left(2^{10}\right)^{202} \times 2^6 \equiv 1^{202} \times 2^6 = 64\,[11].$$

Or $64 = 11 \times 5 + 9$*, donc* $2^{2026} \equiv 9\,[11]$*, et le reste de* 2^{2026} *par* 11 *est* 9 *(Théorème 16.4 (ii) du cours 16 [1]).*

2. Par le Théorème 16.5 (i) du cours 16 [1], $2^{2026} + 2 \equiv 9 + 2 = 11 \equiv 0\,[11]$*, donc* $11 \mid 2^{2026} + 2$*.*

8 PPCM

Exercice 24 *1. Calculer* $\mathrm{PPCM}(48, 180)$*.*

2. Déterminer les multiples communs de 48 *et* 180 *compris entre* 1000 *et* 3000*.*

Solution 24

1. Les entiers 48 *et* 180 *sont non nuls, et* $\mathrm{PGCD}(48, 180) = 12$ *(exercice 9). Par le Théorème 16.19 (ii) du cours 16 [1],*

$$\mathrm{PPCM}(48, 180) = \frac{48 \times 180}{12} = 4 \times 180 = 720.$$

Contrôle : $720 = 48 \times 15 = 180 \times 4$ *; avec les décompositions* $48 = 2^4 \times 3$ *et* $180 = 2^2 \times 3^2 \times 5$*, on a aussi* $720 = 2^4 \times 3^2 \times 5$*.*

2. *Par le Théorème 16.19 (i) du cours 16 [1], les multiples communs de* 48 *et* 180 *sont exactement les multiples de* 720. *Or* $720 \times 1 = 720 < 1000$, $720 \times 2 = 1440$, $720 \times 3 = 2160$, $720 \times 4 = 2880$ *et* $720 \times 5 = 3600 > 3000$. *Les multiples communs compris entre* 1000 *et* 3000 *sont donc* 1440, 2160 *et* 2880.

Références

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