Chapter 3 Arithmétique des entiers

Exercice 1 (3.0)

1. Énoncer le théorème de Bézout dans $\mathbb{Z}$.

2. Soit a et b deux entiers naturels premiers entre eux.
Soit $c \in \mathbb{N}$.
Prouver que: $(a|c \text{ et } b|c) \iff ab|c$.

3. On considère le système (S): $\begin{cases} x \equiv 6 \; [17] \\ x \equiv 4 \; [15] \end{cases}$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.

   (a) Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.

   (b) *Déduire des questions précédentes* la résolution dans $\mathbb{Z}$ du système (S).

Solution 1 (3.0)

1. Théorème de Bézout:
Soit $(a, b) \in \mathbb{Z}^2$.
$a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2 \ / \ au + bv = 1$.

2. Soit $(a, b) \in \mathbb{N}^2$. On suppose que $a \wedge b = 1$.
Soit $c \in \mathbb{N}$.

   Prouvons que $ab|c \implies a|c$ et $b|c$.
   Si $ab|c$ alors $\exists k \in \mathbb{Z} \ / \ c = kab$.
   Alors, $c = (kb)a$ donc $a|c$ et $c = (ka)b$ donc $b|c$.
   Prouvons que $(a|c \text{ et } b|c) \implies ab|c$.

   $a \wedge b = 1$ donc $\exists (u, v) \in \mathbb{Z}^2 \ / \ au + bv = 1$. (1)
   De plus $a|c$ donc $\exists k_1 \in \mathbb{Z} \ / \ c = k_1 a$. (2)
   De même, $b|c$ donc $\exists k_2 \in \mathbb{Z} \ / \ c = k_2 b$. (3)
   On multiplie (1) par c et on obtient $cau + cbv = c$.
   Alors, d'après (2) et (3), $(k_2 b)au + (k_1 a)bv = c$, donc $(k_2 u + k_1 v)(ab) = c$ et donc $ab|c$.
   On a donc prouvé que $(a|c \text{ et } b|c) \iff ab|c$.

3. (a) **Première méthode** (méthode générale):
Soit $x \in \mathbb{Z}$.

$$\begin{aligned} x \text{ solution de}(S) &\iff \exists (k, k') \in \mathbb{Z}^2 \text{ tel que } \begin{cases} x = 6 + 17k \\ x = 4 + 15k' \end{cases} \\ &\iff \exists (k, k') \in \mathbb{Z}^2 \text{ tel que } \begin{cases} x = 6 + 17k \\ 6 + 17k = 4 + 15k' \end{cases} \end{aligned}$$

Or $6 + 17k = 4 + 15k' \iff 15k' - 17k = 2$.
Pour déterminer une solution particulière x_0 de (S), il suffit donc de trouver une solution particulière (k_0, k'_0) de l'équation $15k' - 17k = 2$.
Pour cela, cherchons d'abord, une solution de l'équation $15u + 17v = 1$.
17 et 15 sont premiers entre eux.
Déterminons alors un couple (u_0, v_0) d'entiers relatifs tel que $15u_0 + 17v_0 = 1$.
On a : $17 = 15 \times 1 + 2$ puis $15 = 7 \times 2 + 1$.
Alors $1 = 15 - 7 \times 2 = 15 - 7 \times (17 - 15 \times 1) = 15 - 17 \times 7 + 15 \times 7 = 15 \times 8 - 17 \times 7$

Donc $8 \times 15 + (-7) \times 17 = 1$
Ainsi, $16 \times 15 + (-14) \times 17 = 2$.

On peut prendre alors $k'_0 = 16$ et $k_0 = 14$.

Ainsi, $x_0 = 6 + 17 \times k_0 = 6 + 17 \times 14 = 244$ est une solution particulière de (S).

Deuxième méthode:
En observant le système (S), on peut remarquer que $x_0 = -11$ est une solution particulière.
Cette méthode est évidemment plus rapide mais ne fonctionne pas toujours.

(b) x_0 solution particulière de (S) donc $\left\{ \begin{array}{lcll} x_0 & = & 6 & [17] \\ x_0 & = & 4 & [15] \end{array} \right.$.

On en déduit que x solution de (S) si et seulement si $\left\{ \begin{array}{lcll} x - x_0 & = & 0 & [17] \\ x - x_0 & = & 0 & [15] \end{array} \right.$

c'est-à-dire x solution de $(S) \iff \big(17 | x - x_0$ et $15 | x - x_0\big)$.
Or $17 \wedge 15 = 1$ donc d'après 2., x solution de (S) $\iff (17 \times 15) | x - x_0$.
Donc l'ensemble des solutions de (S) est $\left\{ x_0 + 17 \times 15k,\ k \in \mathbb{Z} \right\} = \{244 + 255k,\ k \in \mathbb{Z}\}$.

Exercice 2 (3.1)

> Démontrer que pour tout $n \in \mathbb{N}$, 7 divise $3^{6n} - 6^{2n}$.

Solution 2 (3.1)

On peut effectuer une récurrence sur $n \in \mathbb{N}$. En effet, 7 divise $0 = 3^0 - 6^0$.

Soit $n \in \mathbb{N}$. Supposons que 7 divise $3^{6n} - 6^{2n}$, c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que

$$3^{6n} - 6^{2n} = 7k.$$

Ainsi $3^{6n} = 6^{2n} + 7k$, d'où

$$3^{6n+6} - 6^{2n+2} = 3^6(6^{2n} + 7k) - 6^{2n+2} = 6^{2n}(3^6 - 6^2) + 7k \times 3^6 = 7\left(99 \times 6^{2n} + 3^6 k\right).$$

Ainsi, 7 divise $3^{6n+6} - 6^{2n+2}$.

On en déduit le résultat par récurrence.

Variante. En utilisant les opération modulo 7:

$$3^3 = 27 \equiv -1 \pmod 7 \text{ donc } 3^6 \equiv (-1)^2 \equiv 1 \pmod 7$$

de même

$$6^2 = 36 \equiv 1 \pmod 7.$$

Ainsi, pour $n \in \mathbb{N}$,

$$3^{6n} - 6^{2n} \equiv 1^n - 1^n \equiv 0 \pmod 7,$$

c'est-à-dire que 7 divise $3^{6n} - 6^{2n}$.

Exercice 3 (3.1)

Les nombres a, b, c, d étant des éléments non nuls de $\mathbb{Z}$, dire si les propriétés suivantes sont vraies ou fausses, en justifiant la réponse.

1. Si a divise b et c, alors $c^2 - 2b$ est multiple de a.
2. Si a divise $b + c$ et $b - c$, alors a divise b et a divise c.
3. Si a est multiple de b et si c est multiple de d, alors $a + c$ est multiple de $b + d$.
4. Si 4 ne divise pas bc, alors b ou c est impair.
5. Si a divise b et b ne divise pas c, alors a ne divise pas c.

Solution 3 (3.1)

1. Vrai. Si a divise b et c, alors a divise $2b$ et $c \times c$ et donc divise $c^2 - 2b$.
2. Faux. On peut montrer que a divise $2b$ et $2c$, ce qui suggère un contre exemple avec $a = 2$. On a bien $a = 2$ qui divise $8 = 5 + 3$ et divise $2 = 5 - 3$ et pourtant 2 ne divise pas 5 (ni 3 d'ailleurs).
3. Faux. $4 = 2 \times 3$ et $35 = 5 \times 7$ et $4 + 35 = 39$ n'est pas multiple de $3 + 7 = 10$.
4. Vrai. On montre facilement la contraposée. Si b et c sont pairs, alors $2 \mid b$ et $2 \mid c$, donc $4 = 2 \times 2 \mid bc$.
5. Faux. $a = 2$ divise $b = 6$ et 6 ne divise pas $c = 10$ et on a bien $2 \mid 10$.

Exercice 4 (3.1)

Déterminer l'ensemble E des $n \in \mathbb{Z}$ tels que $n^2 + 7 \,\Big|\, n^3 + 5$.

Solution 4 (3.1)

Exercice 5 (3.1)

Sachant que l'on a $96842 = 256 \times 375 + 842$, déterminer, sans faire la division, le reste de la division du nombre 96842 par chacun des nombres 256 et 375.

Solution 5 (3.1)

On a $842 = 256 \times 3 + 74$, d'où

$$96842 = 256 \times 375 + 256 \times 3 + 74 = 256 \times 378 + 74 \text{ et } 0 \leq 74 < 256.$$

Le quotient et le reste de la division euclidienne de 96842 par 256 sont respectivement 378 et 74.

De manière analogue, on On a $842 = 2 \times 375 + 92$, d'où

$$96842 = 256 \times 375 + 2 \times 375 + 92 = 258 \times 375 + 92 \text{ et } 0 \leq 92 < 375.$$

Le quotient et le reste de la division euclidienne de 96842 par 375 sont respectivement 258 et 92.

Exercice 6 (3.2)

Résoudre l'équation $xy + 6x - 3y = 40$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

Solution 6 (3.2)
Pour $(x, y) \in \mathbb{Z}^2$,

$$xy + 6x - 3y = 40 \iff (x-3)(y+6) + 18 = 40 \iff (x-3)(y+6) = 22.$$

Or l'ensemble des diviseurs (dans $\mathbb{Z}$) de 22 sont $\{ \pm 1, \pm 2, \pm 11, \pm 22 \}$. On distingue ainsi huit cas:

$$\begin{gathered}
x-3 = 1 \text{ et } y+6 = 22 \iff x = 4 \text{ et } y = 16 \\
x-3 = 2 \text{ et } y+6 = 11 \iff x = 5 \text{ et } y = 5 \\
x-3 = 11 \text{ et } y+6 = 2 \iff x = 14 \text{ et } y = -4 \\
x-3 = 22 \text{ et } y+6 = 1 \iff x = 25 \text{ et } y = -5 \\
x-3 = -1 \text{ et } y+6 = -22 \iff x = 2 \text{ et } y = -28 \\
x-3 = -2 \text{ et } y+6 = -11 \iff x = 1 \text{ et } y = -17 \\
x-3 = -11 \text{ et } y+6 = -2 \iff x = -8 \text{ et } y = -8 \\
x-3 = -22 \text{ et } y+6 = -1 \iff x = -19 \text{ et } y = -7
\end{gathered}$$

L'ensemble des solutions de l'équation $xy + 6x - 3y = 40$ est

$$\{ (4, 16), (5, 5), (14, -4), (25, -5), (2, -28), (1, -17), (-8, -8), (-19, -7) \} .$$

Exercice 7 (3.3)

Calculer pgcd(424, 68) par l'algorithme d'Euclide.

Solution 7 (3.3)
On a successivement

$$\begin{aligned} 424 &= 6 \times 68 + 16 & \text{donc } 424 \mod 68 &= 16 \\ 68 &= 4 \times 16 + 4 & \text{donc } 68 \mod 16 &= 4 \\ 16 &= 4 \times 4 + 0 & \text{donc } 16 \mod 4 &= 0. \end{aligned}$$

Ainsi $\mathrm{pgcd}(424, 68) = 4$.

Exercice 8 (3.3)

Soit $n \in \mathbb{N}$. Déterminer, en discutant éventuellement suivant les valeurs de n, le pgcd des entiers suivants.

$$A = 9n^2 + 10n + 1 \qquad \text{et} \qquad B = 9n^2 + 8n - 1.$$

Solution 8 (3.3)

$$\operatorname{pgcd}(A, B) = \operatorname{pgcd}(A - B, B) = \operatorname{pgcd}(2n + 2, 9n^2 + 8n - 1).$$

En remarquant que $9n^2 + 8n - 1 = (n + 1)(9n - 1)$, on a donc

$$\operatorname{pgcd}(A, B) = \operatorname{pgcd}(2(n + 1), (n + 1)(9n - 1)) = (n + 1) \operatorname{pgcd}(2, 9n - 1) = (n + 1) \operatorname{pgcd}(2, n - 1)$$

puisque $9n - 1 = 2(4n) + n - 1$. Finalement

$$\operatorname{pgcd}(A, B) = \begin{cases} 2(n + 1) & : n \text{ impair} \\ (n + 1) & : n \text{ pair} \end{cases}$$

Exercice 9 (3.3)

On considère l'équation $(E)\ :\ 26x + 15y = 1$ dans laquelle les inconnues x et y sont des entiers relatifs.

1. Écrire l'algorithme d'Euclide pour les nombres 26 et 15.
2. En déduire une solution particulière de (E) puis l'ensemble des solutions de (E).
3. Utiliser ce qui précède pour résoudre l'équation $26x + 15y = 4$.

Solution 9 (3.3)

1. On a

$$26 = 1 \times 15 + 11 \qquad 15 = 1 \times 11 + 4 \qquad 11 = 2 \times 4 + 3 \qquad 4 = 1 \times 3 + 1 \qquad 3 = 3 \times 1 + 0.$$

   Donc $\mathrm{pgcd}(26, 15) = 1$.

2. On remonte les calculs précédents:

$$\begin{aligned} 1 &= 4 - 1 \times 3 & &= 3 \times 4 - 1 \times 11 \because 3 & &= 11 - 2 \times 4 \\ &= 3 \times 15 - 4 \times 11 & &\because 4 = 15 - 1 \times 11 & & \\ &= 7 \times 15 - 4 \times 26 & &\because 11 = 26 - 1 \times 15 & & \end{aligned}$$

   D'où la solution particulière $(x_0, y_0) = (-4, 7)$.

   On a donc

$$26x + 15y = 1 \iff 26x + 15y = 26 \times (-4) + 15 \times 7 \iff 26(x + 4) = -15(y - 7)$$

   Or $15 = 3 \times 5$ est premier avec 26, donc 3 et 5 n'apparaissent pas dans la décomposition en facteurs premiers de 26. On en déduit que 15 divise $x + 4$ dons l'équation précédente. Plus précisement, en posant $x + 4 = 15m$ ($m \in \mathbb{Z}$), nous avons $y - 7 = -26m$.

   Nous pouvons alors vérifier que l'ensemble des solutions de (E) est l'ensemble des couples

$$(15m - 4, -26m + 7) \quad \text{lorsque } m \text{ décrit } \mathbb{Z}.$$

3. Une solution particulière de $26x + 15y = 4$ est $(x_0, y_0) = (-16, 28)$. Un raisonnement analogue au précédent donne tous les couples de solutions $(15m - 16, -26m + 28)$, où $m \in \mathbb{Z}$.

Exercice 10 (3.3)

Les nombres a, b étant des éléments non nuls de $\mathbb{Z}$, dire si les propriétés suivantes sont vraies ou fausses, en justifiant la réponse.

1. Si 19 divise ab, alors 19 divise a ou 19 divise b.
2. Si 91 divise ab, alors 91 divise a ou 91 divise b.
3. Si 5 divise b^2, alors 25 divise b^2.
4. Si 12 divise b^2, alors 4 divise b.
5. Si 12 divise b^2, alors 36 divise b^2.

Solution 10 (3.3)

1. Vrai. 19 est un nombre premier : c'est le lemme d'Euclide.
2. Faux. $91 = 7 \times 13$ n'est pas premier. Avec $a = 7$ et $b = 13$, on a bien $91|ab$ mais 91 ne divise ne a, ni b.
3. Vrai. 5 est premier et $5|b \times b$, donc (lemme d'Euclide) $5|b$, d'où $25|b^2$.
4. Faux. Avec $b = 6$, on a bien $12|b^2$ mais 4 ne divise pas $b^2 = 36$.
5. On écrit la décompostion en facteur premiers de b:

$$b = 2^u 3^v p_1^{\alpha_1} \dots p_r^{\alpha_r}$$

où $2, 3, p_1, \dots, p_r$ sont des nombre premiers distincts, $u \in \mathbb{N}$, $v \in \mathbb{N}$ (donc éventuellement nuls), $\alpha_i \in \mathbb{N}^\star$. On a donc

$$b^2 = 2^{2u} 3^{2v} p_1^{2\alpha_1} \dots p_r^{2\alpha_r}$$

Si $12|b^2$ alors $2|b^2$ et $3|b^2$, donc $2u \geq 1$ et $2v \geq 1$, et puisque $v \in \mathbb{N}$, $2v \geq 2$, donc $12 = 2^1 \times 3^2 | b^2$.

Exercice 11 (3.3)

Résoudre dans $\mathbb{Z}^2$ les équations

1. $1260x + 294y = 3814$.

2. $1260x + 294y = 2814$.

Solution 11 (3.3)

Exercice 12 (3.4)

Combien 15! admet-il de diviseurs positifs ?

Solution 12 (3.4)
On écrit la décompostion en facteurs premiers de 15!:

$$\begin{aligned}
15! &= 2\times 3\times 4\times 5\times 6\times 7\times 8\times 9\times 10\times 11\times 12\times 13\times 14\times 15\\
&= 2\times 3\times 2^2\times 5\times 2\times 3\times 7\times 2^3\times 3^2\times 2\times 5\times 11\times 2^2\times 3\times 13\times 2\times 7\times 3\times 5\\
&= 2^{11}3^6 5^3 7^2 11^1 13^1.
\end{aligned}$$

Les diviseurs positifs de 15! sont donc les entiers de la forme

$$2^a 3^b 5^c 7^d 11^e 13^f \quad \text{avec} \quad \begin{cases} 0\leq a\leq 11\\ 0\leq b\leq 6\\ 0\leq c\leq 3\\ 0\leq d\leq 2\\ 0\leq e\leq 1\\ 0\leq f\leq 1\end{cases}$$

Il y en a donc $12\cdot 7\cdot 4\cdot 3\cdot 2\cdot 2 = 4032$.

Exercice 13 (3.5)

Calculer 2000^{2000} modulo 7 et 2^{500} modulo 3.

Solution 13 (3.5)
On a $2000 = 285 \times 7 + 5$, d'où

$$\begin{aligned}
2000 &\equiv 5 \pmod 7\\
2000^2 &\equiv 5^2 \equiv 25 \equiv 4 \pmod 7\\
2000^3 &\equiv 5 \times 4 \equiv 20 \equiv 6 \pmod 7\\
2000^4 &\equiv 5 \times 6 \equiv 30 \equiv 2 \pmod 7\\
2000^5 &\equiv 5 \times 2 \equiv 10 \equiv 3 \pmod 7\\
2000^6 &\equiv 5 \times 3 \equiv 15 \equiv 1 \pmod 7
\end{aligned}$$

De plus, $2000 = 333 \times 6 + 2$, d'où

$$2000^{2000} = 2000^{333\times6+2} = \left(2000^6\right)^{333} \times 2000^2 \equiv 1^{333}4 \pmod 7 \equiv 4 \pmod 7.$$

De manière analogue, on trouve $2^2 \equiv 1 \pmod 3$, d'où

$$2^{500} = \left(2^2\right)^{250} \equiv 1^{250} \equiv 1 \pmod 3.$$

Exercice 14 (3.5)

Quel est le reste de la division euclidienne de 3^{2022} par 11.

Solution 14 (3.5)
On a successivement,

$$3 \equiv 3 \pmod{11} \quad 3^2 \equiv 9 \pmod{11} \quad 3^3 \equiv 5 \pmod{11} \quad 3^4 \equiv 4 \pmod{11} \quad 3^5 \equiv 1 \pmod{11}.$$

De plus, $2015 = 403 \times 5$, d'où

$$3^{2015} = \left(3^5\right)^{403} \equiv 1^{403} \equiv 1 \pmod{11}.$$

Exercice 15 (3.5)

15 pirates chinois se partagent un butin constitué de pièces d'or. Mais une fois le partage (équitable) effectué, il reste 3 pièces. Que va-t-on en faire ? La discussion s'anime. Bilan : 8 morts. Les 7 survivants recommencent le partage, et il reste cette fois ci 2 pièce ! Nouvelle bagarre à l'issue de laquelle il ne reste que 4 pirates. Heureusement, ils peuvent cette fois ci se partager les pièces sans qu'il n'en reste aucune.
Sachant que 32 Tsing-Tao (bière chinoise) coûtent une pièce d'or, combien (au minimum) de Tsing-Tao pourra boire chaque survivant ?

Solution 15 (3.5)

Exercice 16 (3.5)

Déterminer les nombres entiers x tels que $x^2 - 2x + 2$ soit divisible par 17.

Solution 16 (3.5)
Résumons sous forme de tableau

$x \mod 17$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$x^2 \mod 17$	0	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1
$x^2 - 2x + 2 \mod 17$	2	1	2	5	10	0	9	3	16	14	14	16	3	9	0	10	5

Ainsi $x^2 - 2x + 2$ est divisible par 17 si, et seulement si

$$x \equiv 5 \pmod{17} \text{ ou } x \equiv 14 \pmod{17}.$$

Exercice 17 (3.5)

Soient $a \in \mathbb{N}^\star$ et N le nombre de diviseurs positifs de a. Déterminer une condition nécessaire et suffisante portant uniquement sur N pour que a soit un carré parfait.

Solution 17 (3.5)

N impair.