

Corrigé de la liste d'exercices n°10

Arithmétique

Exercice 1.

1. On a $100 = 2^2 \times 5^2$.

Ainsi, l'ensemble des diviseurs positifs de 100 est $\{2^\alpha 5^\beta, (\alpha, \beta) \in \llbracket 0, 2 \rrbracket^2\}$. Il y en a donc 9 qui sont $\{1, 2, 4, 5, 10, 20, 25, 50, 100\}$.

2. On a $6000000 = 6 \times 10^6 = 2 \times 3 \times (2 \times 5)^6 = 2^7 \times 3 \times 5^6$.

Le nombre 6000000 admet donc $(7+1) \times (1+1) \times (6+1) = 112$ diviseurs positifs.

3. On a

$$13! = 13 \times (2^2 \times 3) \times 11 \times (2 \times 5) \times (3^2) \times (2^3) \times 7 \times (2 \times 3) \times 5 \times 2^2 \times 3 \times 2 = 2^{10} \times 3^5 \times 5^2 \times 7 \times 11 \times 13$$

donc $13!$ admet $(10+1) \times (5+1) \times (2+1) \times (1+1) \times (1+1) \times (1+1) = 1584$ diviseurs positifs.

Le nombre total de diviseurs (positifs ou négatifs) de $13!$ est donc $1584 \times 2 = 3168$.

Exercice 2.

On cherche le nombre d'entiers $k \in \mathbb{N}$ tels que $101 < 7k < 1001$, ce qui équivaut à

$$14 = \frac{98}{7} < \frac{101}{7} < k < \frac{1001}{7} = 143$$

donc $15 \leq k \leq 142$.

Il y a donc $142 - 15 + 1 = 128$ tels entiers.

Exercice 3.

1. Vrai car dans ce cas a divise $bu + cv$ pour tout $(u, v) \in \mathbb{Z}^2$.

2. Vrai pour la même raison.

3. Non, ceci signifie seulement que $\text{pgcd}(a, b)$ divise 4.

Par exemple, si $a = b = 1$, on a $\text{pgcd}(a, b) = 1$ et $2a + 2b = 4$.

4. Vrai : supposons qu'il existe un nombre premier qui divise a et b^3 . Alors p divise $b \times b \times b$ donc p divise b , et a , ce qui est impossible car a et b sont premiers entre eux. Ainsi, le seul diviseur positif commun à a et à b^3 est 1 donc a et b^3 sont premiers entre eux.

5. Faux : un contre-exemple est $a = 2$, et $b = c = 1$.

6. Vrai : c'est le théorème de Bézout.

7. Vrai : les hypothèses impliquent que $|a| \leq |b| \leq |c| \leq |a|$ d'où le résultat.

8. Vrai : c'est une conséquence du lemme de Gauss car 19 est un nombre premier.

9. Faux : si $b = d = 1$, ceci signifierait que tous les entiers sont pairs !

10. Vrai : par hypothèse, il existe $(k, l) \in \mathbb{Z}^2$ tels que $c = ak$ et $d = bl$, donc $cd = (ab)(kl)$.

11. Faux : un contre-exemple est $a = b = 3$.

12. Vrai car b et c divisent bc .

13. Vrai : on a vu en cours que si a divise b , alors $\text{ppcm}(a, b) = |b|$. Réciproquement, si $\text{ppcm}(a, b) = |b|$, alors b est un multiple de a donc a divise b .

14. Faux si $a = \pm 1$. Vrai dans les autres cas car on aurait alors $\text{pgcd}(a, b) = |a| \geq 2$.

15. Faux : si $a = 4$ et $b = 6$, alors $\text{pgcd}(a, b) = 2$ mais a ne divise pas b et b ne divise pas a .
16. Vrai : Montrons-le par contraposée, i.e. montrons que si b et c sont pairs, alors 4 divise bc . En effet, dans ce cas, il existe $(b', c') \in \mathbb{Z}^2$ tels que $b = 2b'$ et $c = 2c'$ donc $bc = 4b'c'$.
17. Faux : un contre-exemple est $a = c = 1$ et $b = 2$.
18. Vrai : puisque 5 divise $b \times b$ et que 5 est premier, alors 5 divise b . Ainsi, il existe $k \in \mathbb{Z}$ tel que $b = 5k$ donc $b^2 = 25k^2$.
19. Faux : un contre-exemple est $b = 6$.
20. Vrai : si $12 = 2^2 \times 3$ divise b^2 , alors 2 et 3 divisent b^2 . Puisque 2 et 3 sont premiers, on en déduit que 2 et 3 divisent b . Or, 2 et 3 sont premiers entre eux donc $2 \times 3 = 6$ divise b , ce qui implique que $6^2 = 36$ divise b^2 .
21. Faux : un contre-exemple est $a = 7$ et $b = 13$.

Exercice 4.

1. Effectuons l'algorithme d'Euclide.

$$\begin{aligned} 9n + 15 &= 2(4n + 7) + (n + 1) \\ 4n + 7 &= 4(n + 1) + 3 \end{aligned}$$

Ainsi $\text{pgcd}(9n + 15, 4n + 7)$ divise 3 donc vaut 1 ou 3.

- Si 3 divise $n + 1$, alors $\text{pgcd}(9n + 15, 4n + 7) = 3$.
 - Si 3 ne divise pas $n + 1$, alors $\text{pgcd}(9n + 15, 4n + 7) = 1$.
2. Supposons par l'absurde qu'il existe un diviseur commun premier p à n^2 et $2n + 1$.
Puisque p est premier et divise n^2 , alors p divise n et $2n + 1$. Ainsi, p divise n et $2n + 1$ donc divise $2n + 1 - 2n = 1$, ce qui est absurde pour un nombre premier.
On en déduit que n^2 et $2n + 1$ ne possèdent pas de facteur premier commun, ce qui implique que n^2 et $2n + 1$ sont premiers entre eux.

Exercice 5.

1. On a $P(41) = 41^2$ qui n'est pas un nombre premier donc $P(n)$ n'est pas un nombre premier pour tout $n \in \mathbb{N}$.
2. Soit $n \in \mathbb{N}$.

On a les équivalences suivantes :

$$43 \text{ divise } P(n) \Leftrightarrow \exists k \in \mathbb{Z}, 43k = n^2 - n + 41 \Leftrightarrow \exists k \in \mathbb{Z}, 43(k-1) = n^2 - n - 2 \Leftrightarrow 43 \text{ divise } n^2 - n - 2.$$

Or, pour tout $n \in \mathbb{N}$, $n^2 - n - 2 = (n + 1)(n - 2)$.

Puisque 43 est premier, on a l'équivalence

$$43 \text{ divise } n^2 - n - 2 \Leftrightarrow 43 \text{ divise } n + 1 \text{ ou } 43 \text{ divise } n - 2$$

donc finalement

$$43 \text{ divise } P(n) \Leftrightarrow \exists k \in \mathbb{Z}, n = 43k - 1 \text{ ou } n = 43k + 2,$$

ce qui assure qu'il existe une infinité d'entiers n tels que 43 divise $P(n)$.

Exercice 6. Soit n un entier naturel.

1. Montrons que $n(n+1)(n+2)$ est divisible par 6.

Il y a forcément un nombre pair parmi $n, n+1$ ou $n+2$ donc 2 divise $n(n+1)(n+2)$.

De même, un des trois nombres $n, n+1$ ou $n+2$ est forcément un multiple de 3 donc 3 divise $n(n+1)(n+2)$.

Puisque 2 et 3 sont premiers entre eux, on en déduit que $2 \times 3 = 6$ divise $n(n+1)(n+2)$.

2. Montrons que $n(n+1)(n+2)(n+3)$ est divisible par 24.

Comme dans la question précédente, (au moins) un des quatre nombres $n, n+1, n+2$ ou $n+3$ est divisible par 3 donc 3 divise $n(n+1)(n+2)(n+3)$.

De plus, parmi ces quatre nombres : deux sont nécessairement pairs, et un des deux est même un multiple de 4. Ainsi, l'un des quatre est divisible par 2, et un autre est divisible par 4, donc $8 = 4 \times 2$ divise $n(n+1)(n+2)(n+3)$.

Puisque 3 et 8 sont premiers entre eux, on en conclut que $24 = 3 \times 8$ divise $n(n+1)(n+2)(n+3)$.

Exercice 7.

1. Puisque $\text{cpgcd}(a, b)$ divise ca et cb , on en déduit que $\text{cpgcd}(a, b)$ divise $\text{pgcd}(ca, cb)$.

Réciproquement, puisque c divise ca et cb , alors c divise $\text{pgcd}(ca, cb)$.

Par ailleurs, puisque $\text{pgcd}(ca, cb)$ divise ca et cb , on en déduit que $\frac{\text{pgcd}(ca, cb)}{c}$ divise a et b , donc divise $\text{pgcd}(a, b)$. On en déduit que $\text{pgcd}(ca, cb)$ divise $\text{cpgcd}(a, b)$.

Finalement, $\text{cpgcd}(a, b)$ divise $\text{pgcd}(ca, cb)$ et réciproquement, donc

$$|c| \text{pgcd}(a, b) = \text{pgcd}(ca, cb).$$

2. • Si $|a| = |b| = 1$, le résultat est évident.

• Supposons que $|a| \geq 2$ ou $|b| \geq 2$.

Soient $(p_1, \dots, p_r)$ l'ensemble des nombres premiers divisant a ou b .

On a alors $a = \prod_{i=1}^r p_i^{v_{p_i}(a)}$, $b = \prod_{i=1}^r p_i^{v_{p_i}(b)}$, $a^2 = \prod_{i=1}^r p_i^{2v_{p_i}(a)}$ et $b^2 = \prod_{i=1}^r p_i^{2v_{p_i}(b)}$.

Il s'ensuit que

$$\text{pgcd}(a^2, b^2) = \prod_{i=1}^r p_i^{\min(2v_{p_i}(a), 2v_{p_i}(b))} = \prod_{i=1}^r p_i^{2\min(v_{p_i}(a), v_{p_i}(b))} = \left(\prod_{i=1}^r p_i^{\min(v_{p_i}(a), v_{p_i}(b))} \right)^2 = \text{pgcd}(a, b)^2.$$

3. Soit d un diviseur positif commun à b et à c . Puisque c divise a , alors d est un diviseur positif commun à a et à b . Or, $\text{pgcd}(a, b) = 1$, donc on a nécessairement $d = 1$, ce qui prouve que $\text{pgcd}(c, b) = 1$.
4. • Supposons que $\text{pgcd}(a, bc) = 1$. D'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tels que

$$au + (bc)v = 1.$$

En posant $v' = cv \in \mathbb{Z}^2$, on a $au + bv' = 1$, ce qui implique d'après le théorème de Bézout que $\text{pgcd}(a, b) = 1$.

De même, en posant $v'' = bv \in \mathbb{Z}^2$, on a $au + cv'' = 1$, ce qui implique d'après le théorème de Bézout que $\text{pgcd}(a, c) = 1$.

• Supposons que $\text{pgcd}(a, b) = 1$ et $\text{pgcd}(a, c) = 1$.

D'après le théorème de Bézout, il existe $(u, v, k, l) \in \mathbb{Z}^4$ tels que

$$au + bv = 1 \quad \text{et} \quad ak + cl = 1.$$

Si on multiplie ces deux identités de Bézout, on obtient

$$a \underbrace{(aku + ucl + kbv)}_{\in \mathbb{Z}} + bc \underbrace{(lv)}_{\in \mathbb{Z}} = 1$$

et on déduit du théorème de Bézout que $\text{pgcd}(a, bc) = 1$.

5. Supposons que $\text{pgcd}(a, b) = 1$.

- On sait que $\text{pgcd}(a + b, a - b)$ divise $(a + b) + (a - b) = 2a$ et $(a + b) - (a - b) = 2b$ donc $\text{pgcd}(a + b, a - b)$ divise $\text{pgcd}(2a, 2b) = 2\text{pgcd}(a, b) = 2$, ce qui implique que $\text{pgcd}(a + b, a - b)$ est égal à 1 ou à 2.
- On sait que $\text{pgcd}(a + b, ab)$ divise $a(a + b) - ab = a^2$ et $b(a + b) - ab = b^2$ donc $\text{pgcd}(a + b, ab)$ divise $\text{pgcd}(a^2, b^2) = \text{pgcd}(a, b)^2 = 1$, ce qui implique que $\text{pgcd}(a + b, ab) = 1$.

Exercice 8.

- Supposons que n est premier. Puisque $n \geq 10$, il est premier avec tous les nombres premiers inférieurs à 10, donc il est premier avec leur produit (d'après la question 4 de l'exercice précédent).

Ainsi, $\text{pgcd}(n, 2 \times 3 \times 5 \times 7) = \text{pgcd}(n, 210) = 1$.

- Supposons que $\text{pgcd}(n, 210) = 1$. Puisque $210 = 2 \times 3 \times 5 \times 7$, on en déduit que le plus petit nombre premier qui puisse apparaître dans la décomposition en facteurs premiers de n est 11. Or, pour tous nombres premiers p et q supérieurs ou égaux à 11, on a $pq > 100$ donc il ne peut y avoir qu'un nombre premier dans la décomposition en facteurs premiers de n , et celui-ci est nécessairement élevée à la puissance 1, donc n est premier.

Exercice 9.

1. On a $637 = 7^2 \times 13$ et $595 = 5 \times 7 \times 17$ donc $\text{pgcd}(637, 595) = 7$.
2. En divisant par 7, on obtient

$$(E) : 637x + 595y = 91 \Leftrightarrow 91x + 85y = 13.$$

Trouvons une relation de Bézout entre 91 et 85. Pour cela, effectuons tout d'abord l'algorithme d'Euclide :

$$91 = 85 \times 1 + 6$$

$$85 = 6 \times 14 + 1$$

puis remontons l'algorithme d'Euclide :

$$\begin{aligned} 1 &= 85 - 6 \times 14 \\ &= 85 - (91 - 85) \times 14 \\ &= 85 \times 15 - 91 \times 14 \end{aligned}$$

donc en multipliant par 13, on obtient $91 \times (-182) + 85 \times 195 = 13$.

Ainsi, le couple $(x_0, y_0) = (-182, 195)$ est une solution particulière de (E) .

Soit (x, y) une solution de (E) .

On a alors

$$91x + 85y = 91x_0 + 85y_0 \Leftrightarrow 91(x - x_0) = 85(y_0 - y).$$

Ainsi, 85 divise $91(x - x_0)$. Or, 91 et 85 sont premiers entre eux donc d'après le lemme de Gauss, on en déduit que 85 divise $x - x_0$, i.e. il existe $k \in \mathbb{Z}$ tel que $x - x_0 = 85k$, ou encore $x = x_0 + 85k$.

En réinjectant dans $91(x-x_0) = 85(y_0-y)$, on obtient $y_0-y = 91k$ ou encore $y = y_0-91k$.
On en déduit que l'ensemble des solutions est inclus dans $\{(x_0 + 85k, y_0 - 91k), k \in \mathbb{Z}\}$.
Réciproquement, s'il existe $k \in \mathbb{Z}$ tel que $(x, y) = (x_0 + 85k, y_0 - 91k)$, on a alors

$$91x + 85y = 91x_0 + 91 \times 85k + 85y_0 - 85 \times 91k = 91x_0 + 85y_0 = 13.$$

Finalement, l'ensemble des solutions de (E) est

$$\{(-182 + 85k, 195 - 91k), k \in \mathbb{Z}\}.$$

3. Puisque $\text{pgcd}(637, 595) = 7$, alors pour tout $(x, y) \in \mathbb{Z}^2$, 7 divise $637x + 595y$. Or, 7 ne divise pas 143 donc cette équation n'admet pas de solution.

Exercice 10.

▷1ère méthode

• Soit $(a, b) \in \mathbb{N}^2$ tels que $\text{pgcd}(a, b) = 12$ et $\text{ppcm}(a, b) = 480$.

Posons $(a', b') \in \mathbb{N}^2$ tels que $a = 12a'$ et $b = 12b'$. Alors a' et b' sont premiers entre eux donc $\text{ppcm}(a', b') = a'b'$.

On a alors $480 = \text{ppcm}(a, b) = \text{ppcm}(12a', 12b') = 12\text{ppcm}(a', b') = 12a'b'$ donc

$$a'b' = \frac{480}{12} = 40.$$

On cherche donc des couples (a', b') d'entiers naturels premiers entre eux tels que $a'b' = 40$.
Les couples possibles sont

$$(a', b') \in \{(1, 40), (5, 8), (8, 5), (40, 1)\}$$

donc

$$(a, b) = (12a', 12b') \in \{(12, 480), (60, 96), (96, 60), (480, 12)\}.$$

• Réciproquement, on vérifie que tous ces couples conviennent donc les couples cherchés sont

$$\{(12, 480), (60, 96), (96, 60), (480, 12)\}.$$

▷2ème méthode (Eloi)

On a $\text{pgcd}(a, b) = 12 = 2^2 \times 3$ et $\text{ppcm}(a, b) = 480 = 2^5 \times 3 \times 5$ donc les couples possibles sont

$$(a, b) \in \{(2^2 \times 3 \times 5, 2^5 \times 3), (2^5 \times 3, 2^2 \times 3 \times 5), (2^5 \times 3 \times 5, 2^2 \times 3), (2^2 \times 3, 2^5 \times 3 \times 5)\}$$

donc

$$(a, b) \in \{(60, 96), (96, 60), (480, 12), (12, 480)\}.$$

Exercice 11. Considérons pour tout $k \in \llbracket 2, n+1 \rrbracket$, $a_k = (n+1)! + k$.

Pour tout $k \in \llbracket 2, n+1 \rrbracket$, k divise $(n+1)!$ (puisque $k \leq n+1$) et k divise k donc k divise $(n+1)! + k = a_k$. Or, $1 < k < a_k$ donc k est un diviseur strict de a_k , ce qui assure que a_k n'est pas premier.

Ainsi, $a_2, a_3, \dots, a_n, a_{n+1}$ sont n entiers consécutifs qui ne sont pas premiers.

Exercice 12.

Par hypothèse, il existe un entier $n \in \mathbb{N}$ tel que $11p + 1 = n^2$, i.e.

$$11p = n^2 - 1 = (n - 1)(n + 1).$$

Puisque 11 est premier et que 11 divise $(n - 1)(n + 1)$, on en déduit que 11 divise $n - 1$ ou 11 divise $n + 1$. De même, puisque p est premier, p divise $(n - 1)$ ou p divise $n + 1$.

De plus, on a forcément $p \neq 11$ puisque $11^2 + 1 = 122$ n'est pas un carré.

- Si 11 et p divisent $n - 1$, puisque 11 et p sont premiers entre eux, on en déduit que $11p$ divise $n - 1$ donc $11p = n - 1$ et $n + 1 = 1$, ce qui donnerait $n = 0$ et $11p = -1$, ce qui est absurde.

- Si 11 et p divisent $n + 1$, puisque 11 et p sont premiers entre eux, on en déduit que $11p$ divise $n + 1$ donc $11p = n + 1$ et $n - 1 = 1$, ce qui donnerait $n = 2$ et $11p = 2$, ce qui est impossible.

- Si 11 divise $n + 1$ et p divise $n - 1$, puisque $11p = (n - 1)(n + 1)$, on a nécessairement $11 = n + 1$ et $p = n - 1$ donc $n = 10$ et $p = 9$, ce qui est impossible puisque p est premier.

- Si 11 divise $n - 1$ et p divise $n + 1$, puisque $11p = (n - 1)(n + 1)$, on a nécessairement $11 = n - 1$ et $p = n + 1$ donc $n = 12$ et $p = 13$, qui est bien un nombre premier.

L'entier cherché est donc $p = 13$.

Exercice 13. • Si un des entiers a ou b est égal à 1, le résultat est évident.

- Supposons que a et b sont tous deux supérieurs ou égaux à 2.

Décomposons a et b en facteurs premiers. Puisque a et b sont premiers entre eux, ils n'ont aucun facteur premier en commun. Il existe donc des entiers $(r, n) \in \mathbb{N}^2$ avec $r \leq n$, des nombres premiers $p_1, \dots, p_r, p_{r+1}, \dots, p_n$ distincts deux à deux et des entiers $\alpha_1, \dots, \alpha_r, \alpha_{r+1}, \dots, \alpha_n$ non nuls tels que

$$a = \prod_{i=1}^r p_i^{\alpha_i} \quad \text{et} \quad b = \prod_{i=r+1}^n p_i^{\alpha_i}.$$

Par hypothèse, on a alors

$$c^2 = ab = \prod_{i=1}^r p_i^{\alpha_i} \prod_{i=r+1}^n p_i^{\alpha_i} = \prod_{i=1}^n p_i^{\alpha_i}.$$

Ainsi, les diviseurs premiers de c sont $p_1, \dots, p_n$ et on a $c = \prod_{i=1}^n p_i^{v_{p_i}(c)}$ d'où

$$c^2 = \prod_{i=1}^n p_i^{2v_{p_i}(c)}.$$

Par unicité de la décomposition en facteurs premiers, on en déduit que pour tout $i \in \llbracket 1, n \rrbracket$, $\alpha_i = 2v_{p_i}(c)$.

Ainsi, $a = \prod_{i=1}^r p_i^{\alpha_i} = \prod_{i=1}^r p_i^{2v_{p_i}(c)} = \left(\prod_{i=1}^r p_i^{v_{p_i}(c)} \right)^2$ est un carré, et il en est de même pour b .

Exercice 14.

1. On peut prendre par exemple $u = 4$ et $v = -11$.

2. On a $c^{25} = (a^u b^v)^{25} = a^{25u} b^{25v} = a^{25u} (b^{25})^v = a^{25u} (a^9)^v = a^{25u+9v} = a$.

De même, $c^9 = (a^u b^v)^9 = a^{9u} b^{9v} = (a^9)^u b^{9v} = (b^{25})^u b^{9v} = b^{25u+9v} = b$.

3. Soit $x \in \mathbb{Q}$. Il existe des entiers $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ avec p et q premiers entre eux tels que $x = \frac{p}{q}$.

Par hypothèse, il existe $(k, l) \in \mathbb{N}^* \times \mathbb{Z}$ tel que $x^k = l$, i.e. $\frac{p^k}{q^k} = l$, ou encore $p^k = lq^k$.

Ainsi, q divise $p^k = \underbrace{p \times \dots \times p}_{k \text{ fois}}$.

Puisque p et q sont premiers entre eux, d'après le lemme de Gauss, on en déduit que q divise p , mais puisque p et q sont premiers entre eux, ceci n'est possible que si $q = 1$.

Ainsi, $x = p \in \mathbb{Z}$.

4. On a $c = a^u b^v = a^4 b^{-11} = \frac{a^4}{b^{11}} \in \mathbb{Q}$. D'après la question 2, $c^9 = b \in \mathbb{Z}$. D'après la question précédente, ceci implique que $c \in \mathbb{Z}$. Enfin, puisque a et b sont strictement positifs, il en découle que $c \in \mathbb{N}^*$.
5. Si m et n sont premiers entre eux, d'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tels que $mu + nv = 1$. En reprenant les questions précédentes en remplaçant 9 par m et 25 par n , on aboutit à la même conclusion.

Exercice 15.

1. Soit $k \in \llbracket 1, \dots, p-1 \rrbracket$. On a $\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1) \dots (p-k+1)}{k!}$ avec $p-k+1 \in \llbracket 2, p \rrbracket$ donc $p(p-1) \dots (p-k+1) = k! \binom{p}{k}$. Ainsi, p divise $k! \binom{p}{k}$. Or, puisque $1 \leq k \leq p-1$, p est premier avec $k!$ donc d'après le lemme de Gauss, p divise $\binom{p}{k}$.
2. Soient $(a, b) \in \mathbb{Z}^2$. D'après la formule du binôme de Newton,

$$(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$$

$$\text{donc } (a+b)^p - a^p - b^p = \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}.$$

Or, d'après la question précédente, pour tout $k \in \llbracket 1, p-1 \rrbracket$, p divise $\binom{p}{k}$ donc p divise $\sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$, ce qui prouve que p divise $(a+b)^p - a^p - b^p$.

3. $\triangleright$ Montrons par récurrence que pour tout $n \in \mathbb{N}$, p divise $n^p - n$.

• **Initialisation** : Si $n = 0$, $n^p - n = 0$ et p divise 0 donc la propriété est vraie au rang $n = 0$.

• **Hérédité** : Soit $n \in \mathbb{N}$ fixé. On suppose que p divise $n^p - n$. Montrons que p divise $(n+1)^p - (n+1)$.

$$\text{On a } (n+1)^p - (n+1) = ((n+1)^p - n^p - 1^p) + (n^p - n).$$

D'après la question précédente, p divise $(n+1)^p - n^p - 1^p$ et par hypothèse de récurrence, p divise $n^p - n$ donc p divise $((n+1)^p - n^p - 1^p) + (n^p - n) = (n+1)^p - (n+1)$, ce qui prouve la propriété au rang $n+1$.

D'après le principe de récurrence, on en conclut que pour tout $n \in \mathbb{N}$, p divise $n^p - n$.

$\triangleright$ Etendons ce résultat aux entiers négatifs.

Soit $n \in \mathbb{Z}$, avec $n < 0$. Alors $-n \in \mathbb{N}^*$.

$$\text{D'après la récurrence, } p \text{ divise } (-n)^p - (-n) = (-1)^p n^p + n.$$

• Si $p = 2$, ceci signifie que 2 divise $n^2 + n$. Or, 2 divise $-2n$ donc 2 divise $(n^2 + n) - 2n = n^2 - n$, ce qui est la propriété voulue.

• Si p est impair, ceci signifie que p divise $-n^p + n$ donc p divise $n^p - n$, ce qui est la propriété voulue.

Dans tous les cas, pour tout $n \in \mathbb{Z}$, p divise $n^p - n$.

4. Soit $n \in \mathbb{Z}$ un entier non divisible par p . D'après la question précédente, p divise $n^p - n = n(n^{p-1} - 1)$.

Puisque p ne divise pas n , p et n sont premiers entre eux et on déduit du lemme de Gauss que p divise $n^{p-1} - 1$.

Exercice 16. Tout d'abord, la remarque de l'énoncé est vraie d'après la décomposition en facteurs premiers d'un entier naturel.

Soit $l \in \llbracket 1, 2n \rrbracket$. On sait qu'il existe $(k, m) \in \mathbb{N}^2$ tel que $l = 2^k(2m + 1)$.

On a nécessairement $1 \leq 2m + 1 \leq 2n - 1$, i.e. $0 \leq 2m \leq 2n - 2$ d'où $0 \leq m \leq n - 1$.

Ainsi, il existe au maximum n choix possibles pour la valeur de m dans la décomposition d'un entier dans $\llbracket 1, 2n \rrbracket$ sous la forme $2^k(2m + 1)$.

Puisque $\text{Card}(A) = n + 1$, il existe nécessairement deux entiers a et b dans $\llbracket 1, n + 1 \rrbracket$ qui s'écrivent avec le même m sous la forme $a = 2^k(2m + 1)$ et $b = 2^{k'}(2m + 1)$, où $(k, k', m) \in \mathbb{N}^3$ et $k \leq k'$ (quitte à échanger a et b).

Puisque $k \leq k'$, on en déduit que a divise b .