# CORRIGÉ – CHAPITRE 1

## DIVISIBILITÉ ET PRIMALITÉ

### Divisibilité dans $\mathbb{Z}$

**EXERCICE 1** ⋆

1. On utilise la factorisation et les propriétés de divisibilité :

   (a) On constate que :

   $$\begin{aligned} & n^2 + n = 20 \\ \Rightarrow \quad & n(n+1) = 20 \end{aligned}$$

   Or $n$ étant un entier relatif, on en déduit que $n$ divise 20, et fait donc partie de l'ensemble :

   $$\{-20, -10, -5, -4, -2, -1, 1, 2, 4, 5, 10, 20\}$$

   Dans cet ensemble, les seules valeurs possibles de $n$ sont ainsi celles telles que $(n+1)$ divise aussi 20 et pour lesquelles $n(n+1) = 20$. N'ayant que $-5 \times (-4)$ et $4 \times 5$ comme possibilités, on en déduit donc que :

   $$\boxed{n \in \{-5, 4\}}$$

   (b) On procède de la même manière, en constatant que :

   $$\begin{aligned} & n^2 + 2n = 35 \\ \Rightarrow \quad & n(n+2) = 35 \end{aligned}$$

   Or $n$ étant un entier relatif, on en déduit que $n$ divise 35, et fait donc partie de l'ensemble :

   $$\{-35, -7, -5, -1, 1, 5, 7, 35\}$$

   Dans cet ensemble, les seules valeurs possibles de $n$ sont ainsi celles telles que $(n+2)$ divise aussi 35 et pour lesquelles $n(n+2) = 35$, n'ayant que $-7 \times -5 = 35$ et $5 \times 7 = 35$ comme possibilités, on en déduit donc que :

   $$\boxed{n \in \{-7, 5\}}$$

2. On utilise de même la factorisation et les propriétés de divisibilité :

   (a) On constate que :

   $$\begin{aligned} & x^2 = y^2 + 21 \\ \Rightarrow \quad & x^2 - y^2 = 21 \\ \Rightarrow \quad & (x-y)(x+y) = 21 \end{aligned}$$

   Or on ne dispose que de quatre possibilités pour factoriser 21 :

   $$\begin{aligned} 1 \times 21 \qquad & -1 \times -21 \\ 3 \times 7 \qquad & -3 \times (-7) \end{aligned}$$

   Pour la première factorisation, on a donc :

   $$\begin{cases} x - y = 1 \\ x + y = 21 \end{cases} \quad \text{ou} \quad \begin{cases} x + y = 1 \\ x - y = 21 \end{cases}$$

   Ce qui nous donne rapidement :

   $$(x, y) = (11, 10) \quad \text{ou} \quad (x, y) = (11, -10)$$

   En procédant de la même façon pour toutes les factorisations, on trouve enfin :

   $$\boxed{(x, y) \in \{(\pm 11, \pm 10), (\pm 5, \pm 2)\}}$$

(b) On constate que :

$$x^2 - 7xy = 17$$
$$x(x - 7y) = 17$$

Or on ne dispose que de deux possibilités pour factoriser 17 :

$$1 \times 17 \qquad \text{ou} \qquad -1 \times -17$$

Pour la première factorisation, on a donc :

$$\begin{cases} x = 1 \\ x - 7y = 17 \end{cases} \qquad \text{ou} \qquad \begin{cases} x = 17 \\ x - 7y = 1 \end{cases}$$

Ce qui nous donne rapidement :

$$\begin{cases} x = 1 \\ -7y = 16 \end{cases} \qquad \text{ou} \qquad \begin{cases} x = 17 \\ 7y = 16 \end{cases}$$

Or ni 7 ni $-7$ ne divise 16, ce qui rend impossible pour $y$ de prendre une valeur entière. Ainsi cette factorisation ne dispose d'aucune solution. On trouve de la même manière que l'autre factorisation est également sans solution, afin d'en déduire que :

$$\boxed{(x, y) \in \varnothing}$$

## EXERCICE 2 ⋆

Le but de l'exercice est de trouver les valeurs du naturel $n > 4$ pour lesquelles la fraction :

$$\frac{n+17}{n-4} \text{ est un entier.}$$

1. On sait que pour que $\dfrac{n+17}{n-4}$ soit entier, $n-4$ doit diviser $n+17$, or on remarque que :

$$\begin{aligned} \frac{n+17}{n-4} &= \frac{n-4+21}{n-4} \\ &= \frac{n-4}{n-4} + \frac{21}{n-4} \\ &= 1 + \frac{21}{n-4} \end{aligned}$$

Ainsi pour que ce nombre soit entier, 21 doit nécessairement être divisible par $n-4$.

2. Les diviseurs de 21 sont :

$$-21, -7, -3, -1, 1, 3, 7, 21$$

3. D'après la question précédente :

$$n - 4 \in \{-21, -7, -3, -1, 1, 3, 7, 21\}$$

On en déduit donc, sachant que $n > 4$ :

$$\boxed{n \in \{5, 7, 11, 25\}}$$

## EXERCICE 3 ⋆

a) Pour que 6 divise $n+5$, il faut que $n+5$ soit multiple de 6, autrement dit qu'il existe $k \in \mathbb{Z}$ tel que $n + 5 = 6k$, ce qui nous dit donc que :

$$\boxed{n \in \{6k - 5 \mid k \in \mathbb{Z}\}}$$

En effet, tout élément de cet ensemble donne un $n+5$ divisible par 6. La première partie de notre raisonnement nous donne une **contrainte** sur $n$, on doit par la suite vérifier que l'ensemble donné est bien solution.

b) Pour que $n$ divise $n+6$, le nombre suivant doit être un entier :

$$\frac{n+6}{n} = \frac{n}{n} + \frac{6}{n} = 1 + \frac{6}{n}$$

On en déduit alors que $n$ doit être un diviseur de 6, et donc que :

$$\boxed{n \in \{-6, -3, -2, -1, 1, 2, 3, 6\}}$$

c) Pour que $n+3$ divise $n+10$, le nombre suivant doit être un entier :

$$\begin{aligned}\frac{n+10}{n+3} &= \frac{n+3+7}{n+3} \\ &= \frac{n+3}{n+3} + \frac{7}{n+3} \\ &= 1 + \frac{7}{n+3}\end{aligned}$$

On en déduit donc que $n+3$ doit être un diviseur de 7, autrement dit que $n+3$ appartient à l'ensemble $\{-7, -1, 1, 7\}$, ce qui nous permet d'en conclure que :

$$\boxed{n \in \{-10, -4, -2, 4\}}$$

d) Pour que $n+1$ divise $3n+4$, le nombre suivant doit être un entier :

$$\begin{aligned}\frac{3n+4}{n+1} &= \frac{3n+3+1}{n+1} \\ &= \frac{3(n+1)}{n+1} + \frac{1}{n+1} \\ &= 3 + \frac{1}{n+1}\end{aligned}$$

On en déduit donc que $n+1$ doit être un diviseur de 1, autrement dit que $n+1$ appartient à l'ensemble $\{-1, 1\}$, ce qui nous permet d'en conclure que :

$$\boxed{n \in \{-2, 0\}}$$

e) Pour que $2n+1$ divise $6n+12$, le nombre suivant doit être un entier :

$$\begin{aligned}\frac{6n+12}{2n+1} &= \frac{6n+3+9}{2n+1} \\ &= \frac{3(2n+1)}{2n+1} + \frac{9}{2n+1} \\ &= 3 + \frac{9}{2n+1}\end{aligned}$$

On en déduit donc que $2n+1$ doit être un diviseur de 9, autrement dit que $2n+1$ appartient à l'ensemble $\{-9, -3, -1, 1, 3, 9\}$, ce qui nous permet d'en conclure que :

$$\boxed{n \in \{-5, -2, -1, 0, 1, 4\}}$$

f) Pour que $3n+1$ divise $10n-4$, le nombre suivant doit être un entier :

$$\begin{aligned}\frac{10n-4}{3n+1} &= \frac{9n+3+n-7}{3n+1} \\ &= \frac{3(3n+1)}{3n+1} + \frac{n-7}{3n+1} \\ &= 3 + \frac{n-7}{3n+1}\end{aligned}$$

On en déduit donc que $3n+1$ doit être un diviseur de $n-7$. Or si c'est le cas, alors d'après la Proposition 1 du cours, $3n+1$ est nécessairement diviseur de :

$$3 \times (n-7) + (-1) \times (3n+1) = -22 \qquad \text{(car } 3n+1 \text{ se divise lui même)}$$

On sait alors que $3n+1$ appartient à l'ensemble $\{-22, -11, -2, -1, 1, 2, 11, 22\}$, ce qui nous permet de conclure que :

$$\boxed{n \in \{-4, -1, 0, 7\}}$$

On peut vérifier notamment que $3n+1$ ne peut pas être égal à $-22$, $-1$, 2 ou 11, sinon $n$ ne serait pas entier.

## EXERCICE 4 ⋆

1. **Vrai.** Il existe $k$ et $k'$ dans $\mathbb{Z}$ tels que $b = ka$ et $c = k'b$, donc $c = (k'k)a$ avec $k'k \in \mathbb{Z}$ : c'est la transitivité de la Proposition 1 du cours. Ainsi $\boxed{a \text{ divise } c}$.
2. **Faux.** Avec $a = 2$ et $b = c = 1$, on a bien 2 qui divise $b + c = 2$, mais 2 ne divise ni $b$ ni $c$. L'erreur la plus répandue consiste à « distribuer » la divisibilité sur une somme : seule l'implication inverse est vraie.
3. **Vrai.** En écrivant $b = ka$ et $c = k'a$, on obtient $2b - 3c = (2k - 3k')a$ avec $2k - 3k' \in \mathbb{Z}$. C'est le cas particulier $u = 2$, $v = -3$ de la Proposition 1.
4. **Faux.** Avec $a = 6$, $b = 2$ et $c = 3$, l'entier 6 divise $bc = 6$ mais ne divise ni 2 ni 3. L'affirmation devient vraie lorsque $a$ est un nombre premier : c'est exactement le lemme d'Euclide.
5. **Faux.** Avec $a = 2$ et $b = -2$, chacun divise l'autre mais $a \neq b$. En revanche, si $b = ka$ et $a = k'b$, alors $a = kk'a$, donc $kk' = 1$ puisque $a \neq 0$, ce qui impose $k = \pm 1$ : on a toujours $\boxed{a = \pm b}$, et $a = b$ si $a$ et $b$ sont tous deux positifs.
6. **Vrai.** Si $b = ka$, alors $b^2 = k^2a^2$ avec $k^2 \in \mathbb{Z}$, donc $\boxed{a^2 \text{ divise } b^2}$. La réciproque est également vraie, mais beaucoup plus délicate : elle fait l'objet de l'exercice 38.

## EXERCICE 5 ⋆

Soit $n$ un entier naturel.

1. Supposons que $n$ est impair. Autrement dit, il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$, ce qui donne :

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2\underbrace{(2k^2 + 2k)}_{\in\mathbb{Z}} + 1 \\ &= 2k' + 1 \qquad \text{où } k' \in \mathbb{Z} \end{aligned}$$

   Ainsi, on a bien montré que $\boxed{n^2 \text{ est impair}}$.

2. Supposons que $n$ est impair. Autrement dit, il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$, ce qui donne :

$$\begin{aligned} n^2 - 1 &= (2k+1)^2 - 1 \\ &= 4k^2 + 4k \\ &= 4k(k+1) \end{aligned}$$

   Or $k$ ou $k + 1$ est nécessairement pair, et le produit d'un entier pair par n'importe quel autre entier est pair, donc il existe $k' \in \mathbb{Z}$ tel que $k(k + 1) = 2k'$, ce qui donne :

$$n^2 - 1 = 4 \times 2k' = 8k'$$

   On en déduit donc que $\boxed{n^2 - 1 \text{ est divisible par } 8}$.

3. On procède par disjonction de cas :

   - Supposons que $n$ est pair :
     On sait alors qu'il existe $k \in \mathbb{Z}$ tel que $n = 2k$, et donc :

$$\begin{aligned} 3n^4 + 5n + 1 &= 3(2k)^4 + 5 \times 2k + 1 \\ &= 3 \times 16k^4 + 5 \times 2k + 1 \\ &= 48k^4 + 10k + 1 \\ &= 2\underbrace{(24k^4 + 5k)}_{\in\mathbb{Z}} + 1 \end{aligned}$$

     Ce qui justifie que le nombre étudié est impair.

- Supposons que $n$ est impair :
  On sait alors qu'il existe $k \in \mathbb{Z}$ tel que $n = 2k+1$, et donc :

$$\begin{aligned}
3n^4+5n+1 &= 3(2k+1)^4+5(2k+1)+1\\
&= 3(2k+1)^2(2k+1)^2+10k+5+1\\
&= 3(4k^2+4k+1)(4k^2+4k+1)+10k+6\\
&= 3(16k^4+16k^3+4k^2+16k^3+16k^2+4k+4k^2+4k+1)+10k+6\\
&= 3(16k^4+32k^3+24k^2+8k+1)+10k+6\\
&= 48k^4+96k^3+72k^2+24k+3+10k+6\\
&= 48k^4+96k^3+72k^2+34k+8+1\\
&= 2\underbrace{(24k^4+48k^3+36k^2+17k+4)}_{\in\mathbb{Z}}+1
\end{aligned}$$

  Ce qui justifie que le nombre étudié est impair.

Le nombre $3n^4+5n+1$ est donc nécessairement impair, il n'est donc pas divisible par un nombre pair. Or on a vu précédemment que $n(n+1)$ est pair, ce qui justifie que :

$$\boxed{3n^4+5n+1 \text{ n'est jamais divisible par } n(n+1)}$$

4. Soit $n$ un nombre strictement inférieur à 100. On pose $a$ le nombre entier correspondant au chiffre des dizaines de $n$, et $b$ le nombre entier correspondant au chiffre des unités de $n$. On a alors :

$$n = 10a+b$$

Sachant ceci, on constate alors que :

$$\begin{aligned}
n-(a+b) &= 10a+b-a-b\\
&= 9a
\end{aligned}$$

Ce qui justifie qu'on obtient $\boxed{\text{un nombre divisible par 9}}$.

5. Soit $n \in \mathbb{Z}$. On procède par disjonction de cas :
   - Supposons qu'il existe $k \in \mathbb{Z}$ tel que $n = 3k$ :
     Ainsi :

$$n(n^2+5) = 3\underbrace{k((3k)^2+5)}_{\in\mathbb{Z}}$$

     Ce qui justifie que $n(n^2+5)$ est divisible par 3.
   - Supposons qu'il existe $k \in \mathbb{Z}$ tel que $n = 3k+1$ :
     Ainsi :

$$\begin{aligned}
n(n^2+5) &= (3k+1)((3k+1)^2+5)\\
&= (3k+1)(9k^2+6k+1+5)\\
&= (3k+1)(9k^2+6k+6)\\
&= 3\underbrace{(3k+1)(3k^2+2k+2)}_{\in\mathbb{Z}}
\end{aligned}$$

     Ce qui justifie que $n(n^2+5)$ est divisible par 3.
   - Supposons qu'il existe $k \in \mathbb{Z}$ tel que $n = 3k+2$ :
     Ainsi :

$$\begin{aligned}
n(n^2+5) &= (3k+2)((3k+2)^2+5)\\
&= (3k+2)(9k^2+12k+4+5)\\
&= (3k+2)(9k^2+12k+9)\\
&= 3\underbrace{(3k+2)(3k^2+4k+3)}_{\in\mathbb{Z}}
\end{aligned}$$

     Ce qui justifie que $n(n^2+5)$ est divisible par 3.

On a donc prouvé que quel que soit $n \in \mathbb{Z}$, $\boxed{n(n^2+5) \text{ est divisible par } 3}$.

## EXERCICE 6 ⋆⋆

Les quatre récurrences suivent le même schéma : on fait apparaître dans l'expression au rang $k+1$ l'expression au rang $k$, puis on utilise l'hypothèse de récurrence.

1. On note $\mathcal{P}_n$ : « 3 divise $4^n - 1$ ».
   - **Initialisation :** $4^0 - 1 = 0 = 3 \times 0$, donc $\mathcal{P}_0$ est vraie.
   - **Hérédité :** Soit $k \in \mathbb{N}$ tel que $\mathcal{P}_k$ soit vraie : il existe $m \in \mathbb{Z}$ tel que $4^k - 1 = 3m$. Alors :
   $$4^{k+1} - 1 = 4 \times 4^k - 4 + 3 = 4(4^k - 1) + 3 = 4 \times 3m + 3 = 3(4m + 1),$$
   donc $\mathcal{P}_{k+1}$ est vraie.
   - **Conclusion :** Pour tout $n \in \mathbb{N}$, $\boxed{3 \text{ divise } 4^n - 1}$.

2. On note $\mathcal{P}_n$ : « 7 divise $9^n - 2^n$ ». On a $9^0 - 2^0 = 0$, donc $\mathcal{P}_0$ est vraie. Si $9^k - 2^k = 7m$ avec $m \in \mathbb{Z}$, alors :
   $$9^{k+1} - 2^{k+1} = 9 \times 9^k - 2 \times 2^k = 9(9^k - 2^k) + 7 \times 2^k = 7(9m + 2^k),$$
   donc $\mathcal{P}_{k+1}$ est vraie, et par récurrence $\boxed{7 \text{ divise } 9^n - 2^n}$ pour tout $n \in \mathbb{N}$.

3. On note $\mathcal{P}_n$ : « 6 divise $n^3 + 5n$ ». On a $0^3 + 5 \times 0 = 0$, donc $\mathcal{P}_0$ est vraie. Si $k^3 + 5k = 6m$ avec $m \in \mathbb{Z}$, alors :
   $$\begin{aligned}(k+1)^3 + 5(k+1) &= k^3 + 3k^2 + 3k + 1 + 5k + 5 \\ &= (k^3 + 5k) + 3k(k+1) + 6.\end{aligned}$$
   Or $k(k+1)$ est le produit de deux entiers consécutifs, dont l'un est pair : il existe $j \in \mathbb{N}$ tel que $k(k+1) = 2j$, donc $3k(k+1) = 6j$. On obtient $(k+1)^3 + 5(k+1) = 6(m + j + 1)$, et par récurrence $\boxed{6 \text{ divise } n^3 + 5n}$ pour tout $n \in \mathbb{N}$.

4. On note $\mathcal{P}_n$ : « 5 divise $2 \times 4^n + 3 \times 9^n$ ». On a $2 + 3 = 5$, donc $\mathcal{P}_0$ est vraie. Si $2 \times 4^k + 3 \times 9^k = 5m$ avec $m \in \mathbb{Z}$, alors en écrivant $9 = 4 + 5$ :
   $$\begin{aligned}2 \times 4^{k+1} + 3 \times 9^{k+1} &= 4 \times 2 \times 4^k + (4+5) \times 3 \times 9^k \\ &= 4\left(2 \times 4^k + 3 \times 9^k\right) + 15 \times 9^k = 5\left(4m + 3 \times 9^k\right),\end{aligned}$$
   donc par récurrence $\boxed{5 \text{ divise } 2 \times 4^n + 3 \times 9^n}$ pour tout $n \in \mathbb{N}$.

Le chapitre suivant, consacré aux congruences, permettra de démontrer ces quatre résultats en une ligne chacun, sans récurrence.

## EXERCICE 7 ⋆⋆

Soit $n$ un entier naturel.

1. Il suffit de faire apparaître $n + 1$ en facteur. En effet :
   $$\begin{aligned}(n+1)(n+4) &= n^2 + n + 4n + 4 \\ &= n^2 + 5n + 4\end{aligned}$$
   Donc $\boxed{(n^2 + 5n + 4) \text{ est bien divisible par } (n+1)}$. De plus :
   $$\begin{aligned}(n+1)(n+2) &= n^2 + n + 2n + 2 \\ &= n^2 + 3n + 2\end{aligned}$$
   Donc $\boxed{(n^2 + 3n + 2) \text{ est bien divisible par } (n+1)}$.

2. On remarque que :
   $$\begin{aligned}\frac{3n^2 + 15n + 19}{n+1} &= \frac{3n^2 + 3n + 12n + 12 + 7}{n+1} \\ &= \frac{3n^2 + 3n}{n+1} + \frac{12n + 12}{n+1} + \frac{7}{n+1} \\ &= \frac{3n(n+1)}{n+1} + \frac{12(n+1)}{n+1} + \frac{7}{n+1} \\ &= 3n + 12 + \frac{7}{n+1}\end{aligned}$$

Ainsi $3n^2+15n+19$ est divisible par $(n+1)$ si et seulement si 7 est divisible par $(n+1)$, et comme $n$ est un entier naturel, $n+1 \geqslant 1$, donc $(n+1)$ appartient à l'ensemble $\{1\,;7\}$, autrement dit :

$$\boxed{n \in \{0\,;6\}}$$

3. On sait d'après la question 1. que $(n+1)$ divise $(n^2+3n+2)$ pour toute valeur de $n$. Si $(n^2+3n+2)$ divisait $(3n^2+15n+19)$, alors $(n+1)$ diviserait $(3n^2+15n+19)$ par transitivité, ce qui n'est possible, d'après la question 2, que pour $n=0$ ou $n=6$. Il reste à examiner ces deux cas : pour $n=0$, $n^2+3n+2=2$ ne divise pas 19 ; pour $n=6$, $n^2+3n+2=56$ ne divise pas $3\times 36+90+19=217$, car $56\times 3=168$ et $56\times 4=224$. Ainsi :

$$\boxed{(3n^2+15n+19) \text{ n'est jamais divisible par } (n^2+3n+2)}$$

## EXERCICE 8 ⋆⋆

La méthode est celle de l'exercice 2 : on écrit le dividende comme un multiple du diviseur plus une constante, puis on utilise la Proposition 1.

a) On a $(n-2)(n+2)=n^2-4$, donc $n^2+3=(n-2)(n+2)+7$. Si $n-2$ divise $n^2+3$, comme il divise aussi $(n-2)(n+2)$, il divise leur différence 7 ; réciproquement, si $n-2$ divise 7, il divise la somme $(n-2)(n+2)+7$. Ainsi $n-2$ divise $n^2+3$ si et seulement si $n-2\in\{-7\,;-1\,;1\,;7\}$, c'est-à-dire :

$$\boxed{n\in\{-5\,;1\,;3\,;9\}}$$

*Vérification :* pour $n=9$, $n^2+3=84=7\times 12$ ; pour $n=-5$, $n^2+3=28=(-7)\times(-4)$.

b) On a $(n+2)(n+3)=n^2+5n+6$, donc $n^2+5n+11=(n+2)(n+3)+5$. Comme précédemment, $n+2$ divise $n^2+5n+11$ si et seulement si $n+2$ divise 5, soit $n+2\in\{-5\,;-1\,;1\,;5\}$ :

$$\boxed{n\in\{-7\,;-3\,;-1\,;3\}}$$

*Vérification :* pour $n=3$, $n^2+5n+11=35=5\times 7$.

c) On a $n^4+2n^2+7=n^2(n^2+2)+7$, donc $n^2+2$ divise $n^4+2n^2+7$ si et seulement si $n^2+2$ divise 7. Comme $n^2+2\geqslant 2$ est positif, cela impose $n^2+2=7$, soit $n^2=5$, ce qui est impossible pour un entier. Il n'y a donc $\boxed{\text{aucune solution}}$.

# Division euclidienne

## EXERCICE 9 ⋆

On pose les divisions euclidiennes :

a) On cherche à diviser 320 par 7 :

| | 3 | 2 | 0 | 7 |
|---|---|---|---|---|
| − | 2 | 8 | ⋮ | 4 5 |
| | | 4 | 0 | |
| − | | 3 | 5 | |
| | | | 5 | |

On a donc $\boxed{320=7\times 45+5}$.

b) On cherche à diviser $-187$ par 7, on s'intéresse donc à la division de 187 par 7 puis on arrangera afin d'obtenir un reste positif :

| | 1 | 8 | 7 | 7 |
|---|---|---|---|---|
| − | 1 | 4 | ⋮ | 2 6 |
| | | 4 | 7 | |
| − | | 4 | 2 | |
| | | | 5 | |

Ce qui donne :

$$\begin{aligned} & 187 = 7 \times 26 + 5 \\ \Rightarrow \quad & -187 = 7 \times (-26) - 5 \\ & = 7 \times (-26) - 5 + 7 - 7 \\ & = 7 \times (-27) + 2 \end{aligned}$$

On a donc $\boxed{-187 = 7 \times (-27) + 2}$.

c) On cherche à diviser 3225 par 11 :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 3 | 2 | 2 | 5 | 1 | 1 | |
| $-$ | 2 | 2 | $\vdots$ | $\vdots$ | 2 | 9 | 3 |
| | 1 | 0 | 2 | $\vdots$ | | | |
| $-$ | | 9 | 9 | $\vdots$ | | | |
| | | | 3 | 5 | | | |
| $-$ | | | 3 | 3 | | | |
| | | | | 2 | | | |

On a donc $\boxed{3225 = 11 \times 293 + 2}$. *Vérification :* $11 \times 293 = 3\,223$ et $3\,225 - 3\,223 = 2$.

d) On cherche à diviser 2024 par 17 :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 2 | 0 | 2 | 4 | 1 | 7 | |
| $-$ | 1 | 7 | $\vdots$ | $\vdots$ | 1 | 1 | 9 |
| | | 3 | 2 | $\vdots$ | | | |
| $-$ | | 1 | 7 | $\vdots$ | | | |
| | | 1 | 5 | 4 | | | |
| $-$ | | 1 | 5 | 3 | | | |
| | | | | 1 | | | |

On a donc $\boxed{2024 = 17 \times 119 + 1}$.

e) On cherche à diviser $-5000$ par 13, on s'intéresse donc à la division de 5000 par 13 puis on arrangera afin d'obtenir un reste positif :

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 5 | 0 | 0 | 0 | 1 | 3 | |
| $-$ | 3 | 9 | $\vdots$ | $\vdots$ | 3 | 8 | 4 |
| | 1 | 1 | 0 | $\vdots$ | | | |
| $-$ | 1 | 0 | 4 | $\vdots$ | | | |
| | | | 6 | 0 | | | |
| $-$ | | | 5 | 2 | | | |
| | | | | 8 | | | |

On a donc :

$$\begin{aligned} & 5000 = 13 \times 384 + 8 \\ \Rightarrow \quad & -5000 = 13 \times (-384) - 8 \\ & = 13 \times (-384) - 8 + 13 - 13 \\ & = 13 \times (-385) + 5 \end{aligned}$$

Ainsi $\boxed{-5000 = 13 \times (-385) + 5}$.

f) On peut vérifier en posant la division que : $\boxed{12345678 = 9 \times 1371742}$.

## EXERCICE 10 ⋆

1. Il existe $q \in \mathbb{N}$ tel que $a = 7q + 3$. Pour chaque nombre, on cherche une écriture $7Q + R$ avec $0 \leqslant R < 7$, et l'unicité de la division euclidienne garantit que $R$ est le reste.
   - $2a = 14q + 6 = 7 \times (2q) + 6$ : le reste est $\boxed{6}$.
   - $a + 5 = 7q + 8 = 7(q + 1) + 1$ : le reste est $\boxed{1}$. Attention, 8 n'est pas un reste possible : il faut « faire passer » 7 dans le quotient.
   - $a^2 = 49q^2 + 42q + 9 = 7(7q^2 + 6q + 1) + 2$ : le reste est $\boxed{2}$.
   - En notant $m = 7q^2 + 6q + 1$, on a $a^3 = a^2 \times a = (7m + 2)(7q + 3) = 49mq + 21m + 14q + 6 = 7(7mq + 3m + 2q) + 6$ : le reste est $\boxed{6}$.
2. D'après ce qui précède, $a^3 + 1 = 7(7mq + 3m + 2q) + 7 = 7(7mq + 3m + 2q + 1)$, donc $\boxed{7 \text{ divise } a^3 + 1}$.

On remarque que ces restes ne dépendent que du reste de $a$, et non de $q$ : c'est l'idée qui fonde les congruences, étudiées au chapitre suivant.

## EXERCICE 11 ⋆

Soient $a$ et $b$ les deux entiers naturels désignés par l'énoncé, tels que $a > b$. On a alors :

$$\begin{cases} a - b = 538 \\ a = 13b + 34 \end{cases}$$

Ce qui donne par combinaison linéaire, en soustrayant la deuxième équation à la première :

$$\begin{aligned} & -b = 538 - 13b - 34 \\ \Rightarrow \quad & 12b = 504 \\ \Rightarrow \quad & b = 42 \end{aligned}$$

Or sachant que $a = 538 + b$, on en déduit que $a = 580$, d'où $\boxed{(a, b) = (580, 42)}$. *Vérification :* $580 = 13 \times 42 + 34$ avec $34 < 42$.

## EXERCICE 12 ⋆

1. On pose $q$ le quotient de la division euclidienne de $n$. On a alors d'après l'énoncé :

   $$\begin{cases} n = 23q + 1 \\ n = 17q + 13 \end{cases}$$

   En soustrayant la deuxième équation à la première, on obtient alors :

   $$\begin{aligned} & 0 = 6q - 12 \\ \Rightarrow \quad & q = 2 \end{aligned}$$

   On en déduit ensuite que $\boxed{n = 47}$.
2. On pose $q$ le quotient de la division euclidienne de $n$. On a alors d'après l'énoncé :

   $$\begin{cases} n = 152q + 13 \\ n = 147q + 98 \end{cases}$$

   En soustrayant la deuxième équation à la première, on obtient alors :

   $$\begin{aligned} & 0 = 5q - 85 \\ \Rightarrow \quad & q = 17 \end{aligned}$$

   On en déduit ensuite que $\boxed{n = 2597}$.

### EXERCICE 13 ⋆⋆

1. On écrit $n = 5q + r$ avec $0 \leqslant r \leqslant 4$. La condition $q = r$ donne $n = 5r + r = 6r$ avec $r \in [\![0; 4]\!]$, donc :

$$\boxed{n \in \{0\,;6\,;12\,;18\,;24\}}$$

   Pour $r = 5$, on aurait $n = 30 = 5 \times 6 + 0$ : le reste n'est plus 5, ce qui explique que la liste s'arrête à 24.

2. On a $1000 = 37b + r$ avec $0 \leqslant r < b$. On en déduit $37b \leqslant 1000 < 37b + b = 38b$, c'est-à-dire :

$$\frac{1000}{38} < b \leqslant \frac{1000}{37}, \qquad \text{soit} \qquad 26{,}3\cdots < b \leqslant 27{,}02\ldots$$

   Le seul entier possible est $b = 27$, et alors $r = 1000 - 37 \times 27 = 1000 - 999 = 1$. Ainsi $\boxed{b = 27 \text{ et } r = 1}$.

3. On a $a = 13 \times 7 + r = 91 + r$ avec $0 \leqslant r \leqslant 12$, donc $\boxed{a \in [\![91; 103]\!]}$, soit treize valeurs.

### EXERCICE 14 ⋆⋆

1. Si $n = 2k$, alors $n^2 = 4k^2$ et le reste est 0. Si $n = 2k + 1$, alors $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$ et le reste est 1. Ainsi $\boxed{\text{le reste de } n^2 \text{ par 4 vaut 0 ou 1}}$.

2. Si $x^2 = 4a + r$ et $y^2 = 4b + s$ avec $r, s \in \{0\,;1\}$, alors $x^2 + y^2 = 4(a + b) + (r + s)$ avec $r + s \in \{0\,;1\,;2\}$. Comme $r + s < 4$, c'est le reste de la division par 4, qui vaut donc 0, 1 ou 2. Or $2023 = 4 \times 505 + 3$ : $\boxed{2023 \text{ n'est pas une somme de deux carrés}}$.

3. On écrit $n = 4k + r$ avec $r \in \{0\,;1\,;2\,;3\}$ :

$$(4k)^2 = 16k^2 = 8 \times 2k^2 + 0, \qquad (4k+1)^2 = 8(2k^2 + k) + 1,$$
$$(4k+2)^2 = 8(2k^2 + 2k) + 4, \qquad (4k+3)^2 = 8(2k^2 + 3k + 1) + 1.$$

   Ainsi $\boxed{\text{le reste de } n^2 \text{ par 8 vaut } 0, 1 \text{ ou } 4}$.

4. Si $x^2 = 8a+r$, $y^2 = 8b+s$ et $z^2 = 8c+t$ avec $r, s, t \in \{0\,;1\,;4\}$, alors $x^2+y^2+z^2 = 8(a+b+c)+(r+s+t)$. Les valeurs possibles de $r + s + t$ sont 0, 1, 2, 3, 4, 5, 6, 8, 9 et 12 ; lorsque la somme dépasse 7, on retire 8 pour obtenir le reste ($8 \to 0$, $9 \to 1$, $12 \to 4$). Les restes possibles sont donc 0, 1, 2, 3, 4, 5 et 6, mais jamais 7. Comme $2023 = 8 \times 252 + 7$, $\boxed{2023 \text{ n'est pas une somme de trois carrés}}$.

Il faut en revanche quatre carrés : $2023 = 1^2 + 2^2 + 13^2 + 43^2$. Lagrange a démontré en 1770 que tout entier naturel est somme de quatre carrés d'entiers.

## Nombres premiers et décomposition en facteurs premiers

### EXERCICE 15 ⋆

On vérifie en testant chaque diviseur premier par une division euclidienne (jusqu'à la racine du nombre étudié), puis on décompose si le reste est nul, et on obtient :

- 97 est un nombre premier.
- 109 est un nombre premier.
- $117 = 3^2 \times 13$
- 271 est un nombre premier.
- 317 est un nombre premier.
- $323 = 17 \times 19$.
- 401 est un nombre premier.
- 419 est un nombre premier.
- $437 = 19 \times 23$.
- $527 = 17 \times 31$.
- 719 est un nombre premier.

## EXERCICE 16 ⋆⋆

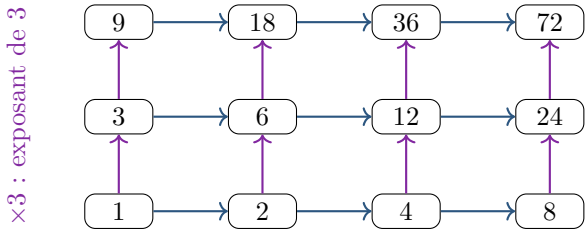
1. En divisant successivement par les nombres premiers dans l'ordre croissant, on obtient :

$$\begin{aligned} 360 &= 2^3 \times 3^2 \times 5, && \text{donc } (3+1)(2+1)(1+1) = 24 \text{ diviseurs;} \\ 1001 &= 7 \times 11 \times 13, && \text{donc } 2 \times 2 \times 2 = 8 \text{ diviseurs;} \\ 2024 &= 2^3 \times 11 \times 23, && \text{donc } 4 \times 2 \times 2 = 16 \text{ diviseurs;} \\ 3600 &= 2^4 \times 3^2 \times 5^2, && \text{donc } 5 \times 3 \times 3 = 45 \text{ diviseurs.} \end{aligned}$$

2. On a $72 = 2^3 \times 3^2$, qui possède $(3+1)(2+1) = 12$ diviseurs :

$$\boxed{1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 12,\ 18,\ 24,\ 36,\ 72}$$

On peut les ranger dans un tableau selon les exposants de 2 et de 3, comme sur la figure ci-dessous.




Chaque case correspond à un unique couple d'exposants $(\beta_1, \beta_2)$ avec $0 \leqslant \beta_1 \leqslant 3$ et $0 \leqslant \beta_2 \leqslant 2$ : on lit sur ce tableau de $4 \times 3$ cases que 72 a bien 12 diviseurs, ce qui illustre la formule du cours.

3. 
- **Sens réciproque.** Si $d = p_1^{\beta_1} \times \cdots \times p_k^{\beta_k}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$, alors $N = d \times m$ avec $m = p_1^{\alpha_1 - \beta_1} \times \cdots \times p_k^{\alpha_k - \beta_k}$, qui est un entier puisque les exposants $\alpha_i - \beta_i$ sont positifs. Donc $d$ divise $N$.
- **Sens direct.** Supposons que $d$ divise $N$ : $N = d \times m$ avec $d$ et $m$ dans $\mathbb{N}^*$. Soit $q$ un facteur premier de $d$. Par transitivité, $q$ divise $N = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$, et en appliquant le lemme d'Euclide autant de fois que nécessaire, $q$ divise l'un des $p_i$. Les deux étant premiers, $q = p_i$. Ainsi les seuls facteurs premiers possibles de $d$, et de même de $m$, sont $p_1$, …, $p_k$, et l'on peut écrire, avec des exposants éventuellement nuls :

$$d = p_1^{\beta_1} \times \cdots \times p_k^{\beta_k} \qquad \text{et} \qquad m = p_1^{\gamma_1} \times \cdots \times p_k^{\gamma_k}.$$

On obtient alors $N = p_1^{\beta_1 + \gamma_1} \times \cdots \times p_k^{\beta_k + \gamma_k}$, et l'unicité de la décomposition donne $\beta_i + \gamma_i = \alpha_i$, donc $\boxed{0 \leqslant \beta_i \leqslant \alpha_i}$ pour tout $i$.

Ce résultat justifie la formule du cours : on choisit chaque $\beta_i$ parmi $\alpha_i + 1$ valeurs, et deux choix différents donnent deux diviseurs différents grâce à l'unicité de la décomposition. Il servira dans les exercices 26, 38, 39 et 41.

## EXERCICE 17 ⋆⋆

Soit $p > 3$ un nombre premier.

1. Si on considère la division euclidienne de $p$ par 12 en notant $q$ on quotient et $r$ son reste, on a alors :

$$p = 12q + r$$

avec $0 \leqslant r < 12$. On élimine les restes impossibles : si $r$ est pair, alors $p = 2(6q) + r$ est pair, donc $p = 2$, ce qui est exclu puisque $p > 3$ ; si $r = 3$ ou $r = 9$, alors $p = 3(4q) + r$ est divisible par 3, donc $p = 3$, ce qui est également exclu ; enfin $r = 0$ donnerait $p = 12q$, divisible par 12. On en déduit donc :

$$\boxed{r \in \{1, 5, 7, 11\}}$$

2. On remarque que :

$$\begin{aligned} p^2 + 11 &= (12q + r)^2 + 11 \\ &= 144q^2 + 24qr + r^2 + 11 \\ &= 12(12q^2 + 2qr) + r^2 + 11 \end{aligned}$$

Ainsi $p^2 + 11$ est divisible par 12 si et seulement si $r^2 + 11$ est divisible par 12, or pour les différentes valeurs possibles de $r$ :

$$\begin{aligned} 1^2 + 11 &= 12 \\ 5^2 + 11 &= 25 + 11 \\ &= 36 = 3 \times 12 \\ 7^2 + 11 &= 49 + 11 \\ &= 60 = 5 \times 12 \\ 11^2 + 11 &= 11(11 + 1) = 11 \times 12 \end{aligned}$$

Ce qui prouve que $\boxed{p^2 + 11 \text{ est divisible par } 12}$.

## EXERCICE 18 ⋆⋆

Déterminer si chacune des affirmations suivantes est **Vraie** ou **Fausse** :

1. $\boxed{\text{Vraie, pour } n = 3}$, en effet :

$$2 \times 3^2 + 3 - 10 = 18 - 7 = 11 \text{ qui est premier}$$

2. $\boxed{\text{Fausse}}$, en effet pour tout $n \in \mathbb{N}$ :

$$\begin{aligned} (2n + 3)(n + 2) &= 2n^2 + 4n + 3n + 6 \\ &= 2n^2 + 7n + 6 \end{aligned}$$

Et par définition de $n$, $(2n + 3)$ et $(n + 2)$ sont des entiers différents de 1.

3. $\boxed{\text{Vraie}}$, en effet, on remarque que pour tout $n \in \mathbb{N}$ :

$$n^2 - 3n + 10 = n(n - 3) + 10$$

Or $n$ ou $n-3$ est nécessairement pair, donc $n(n-3)$ est pair. Le nombre 10 étant également pair, 2 est donc facteur du nombre $n(n - 3) + 10$. De plus, $n^2 - 3n + 10 = \left(n - \frac{3}{2}\right)^2 + \frac{31}{4} \geqslant \frac{31}{4} > 2$ : c'est un nombre pair différent de 2, ce qui justifie que $n^2 - 3n + 10$ n'est pas premier.

4. $\boxed{\text{Fausse}}$, en effet, on pourrait tester jusqu'à trouver un contre exemple, mais en partant de l'idée que l'affirmation est vraie, on peut mettre en évidence ce dernier. Soit $n \in \mathbb{N}$ impair, on sait alors qu'il existe $k \in \mathbb{N}$ tel que $n = 2k + 1$. Ainsi :

$$\begin{aligned} N &= n + (n + 2) + n(n + 2) \\ &= 2k + 1 + (2k + 3) + (2k + 1)(2k + 3) \\ &= 4k + 4 + (4k^2 + 6k + 2k + 3) \\ &= 4k^2 + 12k + 7 \end{aligned}$$

Or on voit ici que si $n = 15$, donc si $k = 7$, alors 7 est facteur de $N$, ce qui prouve que $N$ n'est pas premier. ($n = 9$ est également un contre-exemple)

## EXERCICE 19 ⋆

Notons $N$ le nombre recherché. On utilise dans cet exercice la propriété sur le nombre de diviseurs à partir de la décomposition en facteurs premiers. En effet, on cherche :

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \qquad \text{tel que} \qquad (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1) = 10$$

Or $10 = 2 \times 5$, le produit ne peut donc être que 10 ou $2 \times 5$. On comprend tout d'abord qu'aucun $\alpha_i$ ne peut valoir 9, car sinon $p_i^9$ serait supérieur à 50, ce qui est impossible. Ainsi le produit est nécessairement $2 \times 5$ et on a un $\alpha_i$ qui vaut 1 et l'autre qui vaut 4. Sachant que $3^4 = 81$, ce qui est supérieur à 50, on en déduit que 4 est l'exposant du nombre premier 2, ce qui donne alors :

$$N = 2^4 \times 3^1 = 48$$

Le deuxième nombre premier est nécessairement 3, car $2^4 \times 5^1 = 80 > 50$. On peut donc enfin conclure qu'il n'existe qu'un unique entier contenu entre 0 et 50 qui possède précisément 10 diviseurs, et c'est :

$$\boxed{N = 48}$$

## EXERCICE 20 ⋆⋆

Dans tout l'exercice, on écrit $N = p_1^{\alpha_1} \times \dots \times p_k^{\alpha_k}$ avec des exposants $\alpha_i \geqslant 1$, de sorte que chaque facteur $\alpha_i + 1$ du nombre de diviseurs est au moins égal à 2.

1. Si $(\alpha_1+1) \times \dots \times (\alpha_k+1) = 7$, comme 7 est premier et que chaque facteur vaut au moins 2, il n'y a qu'un seul facteur : $k = 1$ et $\alpha_1 = 6$, donc $N = p^6$. Réciproquement, $p^6$ a bien $6+1 = 7$ diviseurs. Le plus petit est $\boxed{2^6 = 64}$.
2. On a $9 = 9 = 3 \times 3$, donc $N = p^8$ ou $N = p^2q^2$ avec $p < q$ premiers. Le plus petit nombre de la première forme est $2^8 = 256$, celui de la seconde $2^2 \times 3^2 = 36$. Le plus petit entier ayant 9 diviseurs est donc $\boxed{36}$.
3. On a $12 = 12 = 6 \times 2 = 4 \times 3 = 3 \times 2 \times 2$. Pour minimiser $N$, on attribue les plus grands exposants aux plus petits nombres premiers :

   $$p^{11} : 2^{11} = 2048; \qquad p^5q : 2^5 \times 3 = 96; \qquad p^3q^2 : 2^3 \times 3^2 = 72; \qquad p^2qr : 2^2 \times 3 \times 5 = 60.$$

   Le plus petit entier ayant 12 diviseurs est donc $\boxed{60}$.

L'erreur la plus répandue est d'oublier une des factorisations possibles du nombre de diviseurs : ici, c'est la dernière, avec trois facteurs premiers, qui donne le minimum.

## EXERCICE 21 ⋆⋆

On considère un entier $n \in \mathbb{N}$ tel que $n$ a exactement 5 diviseurs, et $(n-16)$ est le produit de deux nombres premiers.

1. On procède comme dans l'exercice 19 pour constater que :

   $$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \qquad \text{tel que} \qquad (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1) = 5$$

   Ainsi, on en déduit qu'un seul élément peut faire partie du produit, et donc que seul $p_1$ est différent de 1, avec $\alpha_1 = 4$. Donc si on note $p = p_1$, on a :

   $$\boxed{n = p^4}$$

2. On constate que :

   $$\begin{aligned} n - 16 = p^4 - 16 &= (p^2-4)(p^2+4) \\ &= \boxed{(p-2)(p+2)(p^2+4)} \end{aligned}$$

3. Sachant que $n-16$ est le produit d'exactement deux nombres premiers, l'un des trois facteurs obtenus à la question précédente vaut nécessairement 1 (pour $p = 2$ on aurait $n - 16 = 0$, donc $p \geqslant 3$ et tous les facteurs sont positifs). Le seul candidat possible est $p-2$, on en déduit donc que $\boxed{p = 3}$ et donc que $\boxed{n = 3^4 = 81}$. *Vérification :* $81 - 16 = 65 = 5 \times 13$, et 81 a bien 5 diviseurs : 1, 3, 9, 27 et 81.

### EXERCICE 22 ⋆

Soient $a$ et $b$ deux entiers tels que $(a^2 - b^2)$ soit un nombre premier.

1. On sait que :

$$a^2 - b^2 = (a - b)(a + b)$$

Or $(a^2 - b^2)$ est premier donc $(a - b)$ vaut nécessairement 1, d'où : $\boxed{a = b + 1}$.

2. 401 n'est divisible par aucun premier inférieur à 23, il est donc premier.

3. D'après la question 1, on a donc :

$$\begin{aligned} & \begin{cases} x + y = 401 \\ x - y = 1 \end{cases} \\ \Rightarrow \quad & 2x = 402 \\ \Rightarrow \quad & x = 201 \end{aligned}$$

On en déduit que $y = 200$, et ainsi $\boxed{(x, y) = (201, 200)}$.

### EXERCICE 23 ⋆⋆

Dans chaque question, on factorise : un produit de deux entiers naturels ne peut être premier que si l'un des facteurs vaut 1.

1. On a $n^2 + 2n - 3 = (n - 1)(n + 3)$. Pour $n = 0$, on obtient $-3$, et pour $n = 1$, on obtient 0, qui ne sont pas premiers. Pour $n \geqslant 2$, les deux facteurs sont positifs et $n + 3 \geqslant 5$, donc le nombre ne peut être premier que si $n - 1 = 1$, soit $n = 2$, qui donne bien 5. Ainsi $\boxed{n = 2}$.

2. On a $n^3 - 1 = (n - 1)(n^2 + n + 1)$. Pour $n \in \{0\,;1\}$, on obtient $-1$ ou 0. Pour $n \geqslant 2$, $n^2 + n + 1 \geqslant 7 > 1$, donc il faut $n - 1 = 1$, soit $n = 2$, qui donne 7, premier. Ainsi $\boxed{n = 2}$.

3. On a $|n^2 - 6n + 8| = |n - 2| \times |n - 4|$. Ce produit est premier si et seulement si l'un des facteurs vaut 1 et l'autre est premier. Si $|n - 2| = 1$, alors $n = 1$, qui donne $1 \times 3 = 3$, premier, ou $n = 3$, qui donne $1 \times 1 = 1$, non premier. Si $|n - 4| = 1$, alors $n = 3$, déjà exclu, ou $n = 5$, qui donne $3 \times 1 = 3$. Ainsi $\boxed{n \in \{1\,;5\}}$.

4. On a $4^n - 1 = (2^n)^2 - 1 = (2^n - 1)(2^n + 1)$. Pour $n = 0$, on obtient 0 ; pour $n = 1$, on obtient 3, premier ; pour $n \geqslant 2$, on a $2^n - 1 \geqslant 3$ et $2^n + 1 \geqslant 5$, donc $4^n - 1$ n'est pas premier. On retrouve d'ailleurs que 3 divise $4^n - 1$ (exercice 6).

## Exercices d'approfondissement

### EXERCICE 24 ⋆⋆⋆

Soit $n$ un entier relatif et $A$ le nombre défini par :

$$A = n^4 - 12n^2 + 16$$

1. On constate que :

$$\begin{aligned} A &= n^4 - 8n^2 + 16 - 4n^2 \\ &= (n^2 - 4)^2 - (2n)^2 \\ &= (n^2 - 4 + 2n)(n^2 - 4 - 2n) \end{aligned}$$

2. Supposons que $n$ est pair, il existe donc $k \in \mathbb{Z}$ tel que $n = 2k$. Ainsi :

$$\begin{aligned} |A| &= |(2k)^4 - 12(2k)^2 + 16| \\ &= |16k^4 - 48k^2 + 16| \\ &= 16 \times |k^4 - 3k^2 + 1| \end{aligned}$$

Or $k^4 - 3k^2 + 1$ ne peut pas être nul pour $k$ entier (on aurait $k^2 = \frac{3 \pm \sqrt{5}}{2}$, qui n'est pas entier), donc $|A| \geqslant 16$ et $|A|$ est divisible par 2 : $\boxed{|A| \text{ n'est pas premier}}$.

3. On suppose que $n$ est impair. On pose alors $n = 2k+1$ avec $k \in \mathbb{Z}$.

(a) On suppose que $n$ est impair, donc qu'il existe $k \in \mathbb{Z}$ tel que $n = 2k+1$. On constate tout d'abord que :

$$\begin{aligned}(4k^2+8k-1)(4k^2-5) &= 4k^2 \times 4k^2 + 4k^2 \times (-5) + 8k \times 4k^2 \\ &\quad + 8k \times (-5) - 4k^2 + 5 \\ &= 16k^4 - 20k^2 + 32k^3 - 40k - 4k^2 + 5 \\ &= 16k^4 + 32k^3 - 24k^2 - 40k + 5\end{aligned}$$

On constate alors de plus que :

$$\begin{aligned}A &= (2k+1)^4 - 12(2k+1)^2 + 16 \\ &= (2k+1)^2(2k+1)^2 - 12(4k^2+4k+1) + 16 \\ &= (4k^2+4k+1)(4k^2+4k+1) - 48k^2 - 48k - 12 + 16 \\ &= 16k^4 + 16k^3 + 4k^2 + 16k^3 + 16k^2 + 4k + 4k^2 + 4k + 1 - 48k^2 - 48k + 4 \\ &= 16k^4 + 32k^3 - 24k^2 - 40k + 5 \\ &= (4k^2+8k-1)(4k^2-5)\end{aligned}$$

(b) $|A|$ est un nombre premier seulement si l'un de ses deux facteurs vaut 1 ou $-1$, donc premièrement si $4k^2+8k-1 = 1$ ou $4k^2-5 = 1$. On a tout d'abord :

$$\begin{aligned}4k^2+8k-1 = 1 \quad &\Rightarrow \quad 4k^2+8k-2 = 0 \\ &\Rightarrow \quad 2k^2+4k-1 = 0\end{aligned}$$

Or cette équation a pour discriminant :

$$\Delta = 4^2 - 4 \times 2 \times (-1) = 25$$

Elle a ainsi deux solutions réelles :

$$k_1 = \frac{-4-5}{2\times 2} = -\frac{11}{4} \qquad \text{et} \qquad k_2 = \frac{-4+5}{2\times 2} = \frac{1}{4}$$

Or aucune des deux n'est entière. De plus la deuxième équation équivaut à $k^2 = \dfrac{3}{2}$, qui n'a manifestement pas non plus de solutions entières.
On regarde deuxièmement $4k^2+8k-1 = -1$ et $4k^2-5 = -1$. On a tout d'abord :

$$\begin{aligned}4k^2+8k-1 = -1 \quad &\Rightarrow \quad 4k^2+8k = 0 \\ &\Rightarrow \quad k(k+2) = 0\end{aligned}$$

On a donc deux solutions entières, $k_1 = 0$ et $k_2 = -2$. De plus la deuxième équation équivaut à $k^2 = 1$, elle donne donc deux solutions entières supplémentaires, $k_3 = 1$ et $k_4 = -1$. On peut enfin en conclure que $|A|$ est premier pour :

$$\boxed{n \in \{-3, -1, 1, 3\}}$$

## EXERCICE 25 : NOMBRES DE MERSENNE ⋆⋆⋆

Soit $n \in \mathbb{N}^*$, on appelle nombre de Mersenne tout nombre $M_n = 2^n - 1$.

1. Pour répondre à cette question, on aura besoin de prouver le résultat suivant :

$$\mathcal{P}_n \ : \ \text{« } \forall n \in \mathbb{N}^*, \qquad a^n - 1 = (a-1)(1 + a + a^2 + \cdots + a^{n-1}) \text{ »}$$

On procède par récurrence :

- **Initialisation :** On constate que :

$$a^1 - 1 = (a-1) \times 1$$

Ainsi $\mathcal{P}_1$ est vraie.

- **Hérédité :** Soit $k \in \mathbb{N}^*$, on suppose que la propriété $\mathcal{P}_k$ est vraie. On a alors :

$$\begin{aligned}(a-1)(1+a+a^2+\cdots+a^k) &= (a-1)(1+a+a^2+\cdots+a^{k-1}+a^k)\\ &= (a-1)(1+a+a^2+\cdots+a^{k-1})+(a-1)\times a^k\\ &= a^k-1+a^{k+1}-a^k\\ &= a^{k+1}-1\end{aligned}$$

  Ce qui prouve donc que $\mathcal{P}_{k+1}$ est vraie.
- **Conclusion :** D'après le principe de récurrence, la propriété $\mathcal{P}_n$ est donc vraie pour tout $n \in \mathbb{N}$.

On déduit ainsi du résultat précédent que si $a^n-1$ est premier, son facteur $(a-1)$ vaut nécessairement 1 et donc $\boxed{a=2}$. Supposons maintenant que $n$ n'est pas premier afin de raisonner par l'absurde. Si $n$ n'est pas premier, alors il existe $p$ et $q$ deux entiers supérieurs ou égaux à 2 tels que $n = p \times q$. Ainsi si on applique le résultat prouvé précédemment, on a :

$$\begin{aligned}a^n-1 &= a^{p\times q}-1\\ &= (a^p)^q-1\\ &= (a^p-1)(1+a^p+a^{2p}+\cdots+a^{p\times(q-1)})\\ &= (a-1)\underbrace{(1+a+a^2+\cdots+a^{p-1})}_{\neq 1}\underbrace{(1+a^p+a^{2p}+\cdots+a^{p\times(q-1)})}_{\neq 1}\end{aligned}$$

Ainsi $a^n-1$ ne serait pas premier, ce qui est absurde, ce qui justifie que $\boxed{n \text{ est premier}}$. Ainsi, un nombre de Mersenne ne peut être premier que si $n$ est premier.

2. Dans cette question, on vérifie que la réciproque est fausse, tout nombre de Mersenne n'est pas premier. En effet :

$$2^{11}-1 = 2047 = 23\times 89$$

Ainsi $\boxed{M_{11} \text{ n'est pas premier}}$.

## EXERCICE 26 : SOMME DES DIVISEURS ⋆⋆⋆

1. D'après l'exercice 16, $\sigma(72) = 1+2+3+4+6+8+9+12+18+24+36+72 = \boxed{195}$, et $(1+2+4+8)(1+3+9) = 15\times 13 = 195$. En développant ce produit, on obtient chacun des termes $2^i3^j$ une et une seule fois, c'est-à-dire chacune des cases du tableau de l'exercice 16.
2. D'après l'exercice 16, les diviseurs de $p^\alpha$ sont $1, p, \ldots, p^\alpha$, donc $\sigma(p^\alpha) = 1+p+\cdots+p^\alpha$. C'est la somme des termes d'une suite géométrique de raison $p \neq 1$ ; on peut aussi utiliser l'identité démontrée dans l'exercice 25, $(p-1)(1+p+\cdots+p^\alpha) = p^{\alpha+1}-1$. Comme $p-1 \neq 0$ :

$$\boxed{\sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}}$$

3. D'après l'exercice 16, les diviseurs de $p^\alpha q^\beta$ sont les $p^iq^j$ avec $0 \leqslant i \leqslant \alpha$ et $0 \leqslant j \leqslant \beta$, et ils sont deux à deux distincts par unicité de la décomposition. Or en développant :

$$(1+p+\cdots+p^\alpha)(1+q+\cdots+q^\beta) = \sum_{i=0}^{\alpha}\sum_{j=0}^{\beta} p^iq^j,$$

on obtient exactement la somme de ces diviseurs, chacun une fois. Donc $\boxed{\sigma(p^\alpha q^\beta) = \sigma(p^\alpha)\times\sigma(q^\beta)}$.

4. Comme $360 = 2^3\times 3^2\times 5$ :

$$\sigma(360) = (1+2+4+8)(1+3+9)(1+5) = 15\times 13\times 6 = \boxed{1170}.$$

5. Pour $n=1$, $\sigma(1) = 1 \neq 2$. Pour $n \geqslant 2$, 1 et $n$ sont deux diviseurs distincts de $n$, donc $\sigma(n) \geqslant n+1$, avec égalité si et seulement si $n$ n'a pas d'autre diviseur, c'est-à-dire si et seulement si $n$ est premier. Ainsi $\boxed{\sigma(n) = n+1 \iff n \text{ est premier}}$.

La fonction $\sigma$ intervient dans la définition des nombres parfaits, étudiés dans l'exercice 41.

## EXERCICE 27 : UNE INFINITÉ DE NOMBRES PREMIERS DE LA FORME $6k+5$ ⋆⋆⋆

1. On écrit $p = 6k + r$ avec $0 \leqslant r \leqslant 5$. Si $r \in \{0\,;2\,;4\}$, alors $p = 2\left(3k + \frac{r}{2}\right)$ est pair, donc $p = 2$, ce qui est exclu puisque $p \geqslant 5$. Si $r = 3$, alors $p = 3(2k+1)$ est divisible par 3, donc $p = 3$, exclu également. Il reste $\boxed{r \in \{1\,;5\}}$.

2. On a $(6a+1)(6b+1) = 36ab+6a+6b+1 = 6(6ab+a+b)+1$. Par récurrence sur $r$ : un seul entier de la forme $6k+1$ convient évidemment, et si un produit de $r$ tels entiers s'écrit $6k+1$, alors en le multipliant par un $(r+1)$-ième entier $6b+1$, on obtient, d'après le calcul précédent, un entier de la forme $6k'+1$.

3. Soit $N = 6k+5$. Il est impair, car $N = 2(3k+2)+1$, et il n'est pas divisible par 3, car $N = 3(2k+1)+2$ et le reste 2 n'est pas nul. Tous ses facteurs premiers sont donc au moins égaux à 5, et sont donc de la forme $6j+1$ ou $6j+5$ d'après la question 1. S'ils étaient tous de la forme $6j+1$, leur produit $N$ serait de la forme $6K+1$ d'après la question 2. Mais l'unicité de la division euclidienne par 6 interdit que $N$ ait à la fois 1 et 5 pour reste. Ainsi $\boxed{N \text{ admet un diviseur premier de la forme } 6k+5}$.

4. L'entier $N = 6p_1 \cdots p_r - 1 = 6(p_1 \cdots p_r - 1) + 5$ est de la forme $6k+5$ (avec $k \geqslant 0$ car $p_1 \cdots p_r \geqslant 5$). D'après la question 3, il admet un diviseur premier de la forme $6k+5$, qui est donc l'un des $p_i$. Mais alors $p_i$ divise $N$ et $6p_1 \cdots p_r$, donc il divise leur différence, qui vaut 1 : c'est absurde. Il existe donc $\boxed{\text{une infinité de nombres premiers de la forme } 6k+5}$.

La démarche est celle de la Proposition 3 du cours. Elle ne s'adapte pas directement aux nombres premiers de la forme $6k+1$ : un entier de la forme $6k+1$ peut n'avoir que des facteurs premiers de la forme $6k+5$, comme $25 = 5 \times 5$. Le théorème de Dirichlet (1837) affirme plus généralement qu'il y a une infinité de nombres premiers de la forme $ak+b$ dès que $a$ et $b$ n'ont pas de diviseur commun autre que $\pm 1$.

## EXERCICE 28 : CRITÈRES DE DIVISIBILITÉ ⋆⋆⋆

1. On a $10^0 - 1 = 0$, divisible par 9. Si $10^k - 1 = 9m$, alors $10^{k+1} - 1 = 10(10^k - 1) + 9 = 9(10m+1)$. Par récurrence, $\boxed{9 \text{ divise } 10^n - 1}$ pour tout $n \in \mathbb{N}$.

2. En regroupant les termes :

$$N - S = a_k(10^k - 1) + a_{k-1}(10^{k-1} - 1) + \cdots + a_1(10-1) + a_0(1-1).$$

Chaque $10^i - 1$ est un multiple de 9 d'après la question 1, donc 9 divise $N - S$ par la Proposition 1. Si 9 divise $S$, il divise $N = (N-S) + S$ ; si 9 divise $N$, il divise $S = N - (N-S)$. Enfin 3 divise 9, donc 3 divise aussi $N - S$ par transitivité, et le même raisonnement montre que 3 divise $N$ si et seulement si 3 divise $S$.

3. La somme des chiffres de 123 456 789 est $1+2+\cdots+9 = 45 = 9 \times 5$, donc 123 456 789 est $\boxed{\text{divisible par 9}}$ ; on trouve d'ailleurs $123\,456\,789 = 9 \times 13\,717\,421$.

4. On note $\mathcal{Q}_n$ : « 11 divise $10^{2n} - 1$ ». On a $10^0 - 1 = 0$. Si $10^{2k} - 1 = 11m$, alors :

$$10^{2k+2} - 1 = 100(10^{2k} - 1) + 99 = 11(100m + 9).$$

Par récurrence, 11 divise $10^{2n} - 1$ pour tout $n$. On en déduit $10^{2n+1} + 1 = 10(10^{2n} - 1) + 11 = 11(10m+1)$, divisible par 11.

5. On a $N - T = \sum_{i=0}^{k} a_i \left(10^i - (-1)^i\right)$. Pour $i$ pair, $10^i - (-1)^i = 10^i - 1$ et pour $i$ impair, $10^i - (-1)^i = 10^i + 1$ : dans les deux cas, c'est un multiple de 11 d'après la question 4. Donc 11 divise $N - T$ et, comme à la question 2 :

$$\boxed{11 \text{ divise } N \iff 11 \text{ divise } T}$$

6. En partant du chiffre des unités, $T = 2 - 8 + 0 - 8 + 1 - 9 = -22 = 11 \times (-2)$, donc 918 082 est $\boxed{\text{divisible par 11}}$ ; en effet $918\,082 = 11 \times 83\,462$.

La question 2 généralise la question 4 de l'exercice 5, qui ne traitait que des nombres à deux chiffres. Avec les congruences du chapitre suivant, ces critères découleront immédiatement de ce que 10 a pour reste 1 dans la division par 9, et $-1$ « modulo 11 ».

## Pour aller plus loin

### EXERCICE 29 ⋆⋆

Soit $n = k(k+1)(k+2)(k+3)$ avec $k \in \mathbb{N}^*$. On regroupe le premier facteur avec le dernier, et les deux du milieu ensemble :

$$k(k+3) = k^2 + 3k \qquad \text{et} \qquad (k+1)(k+2) = k^2 + 3k + 2.$$

En posant $u = k^2 + 3k$, on obtient $n = u(u+2) = u^2 + 2u$, donc :

$$n + 1 = u^2 + 2u + 1 = (u+1)^2 = \boxed{(k^2 + 3k + 1)^2}$$

*Vérification :* pour $k = 1$, $n + 1 = 24 + 1 = 25 = 5^2$ ; pour $k = 2$, $n + 1 = 120 + 1 = 121 = 11^2$. L'énoncé original du poly écrit « $n - 1$ », ce qui est une coquille : $24 - 1 = 23$ n'est pas un carré.

### EXERCICE 30 ⋆⋆

a) On montre l'identité $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$. En effet, en développant, les termes se télescopent :

$$\begin{aligned}(a-b)\sum_{i=0}^{n-1} a^{n-1-i}b^i &= \sum_{i=0}^{n-1} a^{n-i}b^i - \sum_{i=0}^{n-1} a^{n-1-i}b^{i+1} \\ &= \sum_{i=0}^{n-1} a^{n-i}b^i - \sum_{i=1}^{n} a^{n-i}b^i = a^n - b^n.\end{aligned}$$

La somme $\sum a^{n-1-i}b^i$ étant un entier, $\boxed{a - b \text{ divise } a^n - b^n}$. Pour $b = 1$, on retrouve l'identité utilisée dans l'exercice 25 sur les nombres de Mersenne.

b) Si $n$ est impair, $(-b)^n = -b^n$. En appliquant a) aux entiers $a$ et $-b$, on obtient que $a - (-b) = a + b$ divise $a^n - (-b)^n = a^n + b^n$. Ainsi $\boxed{a + b \text{ divise } a^n + b^n}$. Pour $n$ pair, c'est faux en général : $1 + 2 = 3$ ne divise pas $1^2 + 2^2 = 5$.

### EXERCICE 31 ⋆⋆⋆

a) Si $n = mk$ avec $k \in \mathbb{N}^*$, alors $a^n - 1 = (a^m)^k - 1^k$, qui est divisible par $a^m - 1$ d'après l'exercice 30 a). Ainsi $\boxed{a^m - 1 \text{ divise } a^n - 1}$.

b) On écrit $n = mq + r$ avec $0 \leqslant r < m$. Alors :

$$a^n - 1 = a^r\left(a^{mq} - 1\right) + \left(a^r - 1\right).$$

Si $q \geqslant 1$, la question a) donne $a^{mq} - 1 = (a^m - 1)Q$ avec $Q = 1 + a^m + \cdots + a^{m(q-1)}$ ; si $q = 0$, on pose $Q = 0$. On obtient l'identité :

$$\boxed{a^n - 1 = (a^m - 1) \times a^r Q + (a^r - 1)}$$

Comme $a \geqslant 2$ et $0 \leqslant r < m$, on a $1 \leqslant a^r < a^m$, donc $0 \leqslant a^r - 1 < a^m - 1$. Par unicité de la division euclidienne, le quotient de $a^n - 1$ par $a^m - 1$ est $a^r Q$ et le reste est $\boxed{a^r - 1}$.

*Vérification :* pour $a = 2$, $n = 10$, $m = 3$, on a $r = 1$, et en effet $2^{10} - 1 = 1023 = 7 \times 146 + 1$. On en déduit que $a^m - 1$ divise $a^n - 1$ si et seulement si $r = 0$, c'est-à-dire si et seulement si $m$ divise $n$.

## EXERCICE 32 ⋆⋆⋆

1. On a $n^2+1=(n+1)(n-1)+2$. Si $n+1$ divise $n^2+1$, comme il divise $(n+1)(n-1)$, il divise la différence 2 ; réciproquement, s'il divise 2, il divise la somme $(n+1)(n-1)+2$. Comme $n+1 \geqslant 1$, la condition s'écrit $n+1 \in \{1\,;2\}$, soit $\boxed{n \in \{0\,;1\}}$.

2. On cherche à faire apparaître un multiple de $n+3$. D'après l'exercice 30 b), $n+3$ divise $n^3+3^3=n^3+27$, et plus précisément $n^3+27=(n+3)(n^2-3n+9)$. Ainsi :

$$n^3+3=(n+3)(n^2-3n+9)-24.$$

Pour $n=-3$, $n+3=0$ ne divise pas $n^3+3=-24\neq 0$. Pour $n\neq -3$, le même raisonnement qu'à la question 1 montre que $n+3$ divise $n^3+3$ si et seulement si $n+3$ divise 24, c'est-à-dire $n+3 \in \{\pm1,\pm2,\pm3,\pm4,\pm6,\pm8,\pm12,\pm24\}$. On obtient les seize valeurs :

$$\boxed{n \in \{-27,-15,-11,-9,-7,-6,-5,-4,-2,-1,0,1,3,5,9,21\}}$$

*Vérification :* pour $n=21$, $n^3+3=9264=24\times 386$ ; pour $n=-27$, $n^3+3=-19680=(-24)\times 820$.

## EXERCICE 33 ⋆⋆

Soit $p \geqslant 5$ un nombre premier. Il est impair : $p=2a+1$ avec $a \geqslant 2$. On a :

$$p^2-1=(p-1)(p+1)=2a(2a+2)=4a(a+1).$$

L'un des deux entiers consécutifs $a$ et $a+1$ est pair, donc 8 divise $p^2-1$ : il existe $b\in\mathbb{N}$ tel que $p^2-1=8b$. Par ailleurs, en écrivant $p=3q+r$ avec $r\in\{0\,;1\,;2\}$, on a $r\neq 0$ car $p$ est premier et différent de 3. Si $r=1$, 3 divise $p-1$ ; si $r=2$, alors $p+1=3(q+1)$. Dans les deux cas, 3 divise $(p-1)(p+1)=8b$. Comme 3 est premier et ne divise pas 8, le lemme d'Euclide donne que 3 divise $b$ : $b=3c$, d'où $p^2-1=24c$. Ainsi $\boxed{24 \text{ divise } p^2-1}$.
*Vérification :* $5^2-1=24$, $7^2-1=48$, $11^2-1=120=24\times 5$. Ce résultat renforce celui de l'exercice 17, puisque $p^2+11=(p^2-1)+12$.

## EXERCICE 34 : NOMBRES DE FERMAT ⋆⋆⋆

Raisonnons par l'absurde en supposant que $n$ n'est pas une puissance de 2. En regroupant les facteurs 2 de sa décomposition, on écrit $n=2^\alpha m$ avec $m$ impair, et $m\neq 1$ puisque $n$ n'est pas une puissance de 2 : donc $m\geqslant 3$. On pose $k=2^\alpha$, de sorte que $n=km$ et :

$$2^n+1=\left(2^k\right)^m+1^m.$$

Comme $m$ est impair, l'exercice 30 b) montre que $2^k+1$ divise $2^n+1$. Or $k=\frac{n}{m}<n$, donc $1<2^k+1<2^n+1$ : l'entier $2^n+1$ admet un diviseur autre que 1 et lui-même, ce qui contredit le fait qu'il soit premier. Ainsi $\boxed{n \text{ est une puissance de } 2}$.
La réciproque est fausse : $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$ et $F_4=65\,537$, où $F_j=2^{2^j}+1$, sont premiers, mais Euler a montré en 1732 que $F_5=4\,294\,967\,297=641\times 6\,700\,417$. Le résultat est l'analogue « additif » de celui de l'exercice 25 sur les nombres de Mersenne.

## EXERCICE 35 ⋆⋆

a) On complète le carré $x^4+4y^4$ en $(x^2+2y^2)^2=x^4+4x^2y^2+4y^4$ :

$$x^4+4y^4=(x^2+2y^2)^2-(2xy)^2=\boxed{(x^2-2xy+2y^2)(x^2+2xy+2y^2)}.$$

b) D'après a), $m^4+4n^4=(m^2-2mn+2n^2)(m^2+2mn+2n^2)$. Le second facteur vaut au moins 5, et le premier s'écrit $(m-n)^2+n^2\geqslant 1$. Si $m^4+4n^4$ est premier, le premier facteur vaut nécessairement 1, donc $(m-n)^2+n^2=1$ avec $n\geqslant 1$, ce qui impose $n=1$ et $m-n=0$, soit $m=n=1$. Réciproquement, $1^4+4\times 1^4=5$ est premier. Ainsi $\boxed{m^4+4n^4 \text{ premier } \iff m=n=1}$.

En particulier, avec $n=1$, l'entier $m^4+4$ n'est jamais premier pour $m\geqslant 2$, par exemple $3^4+4=85=5\times 17$. Cette factorisation est appelée identité de Sophie Germain.

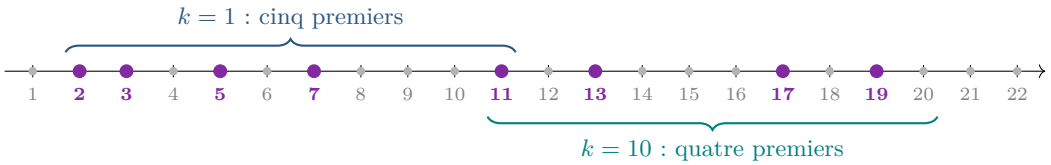
## EXERCICE 36 ⋆⋆⋆

1. Soit $k \in [\![2; n]\!]$. L'entier $k$ figure dans le produit $n! = 1 \times 2 \times \cdots \times n$, donc il divise $n!$, et il divise $k$ : il divise donc $n! + k$. Comme $2 \leqslant k < n! + k$, l'entier $n! + k$ admet un diviseur autre que 1 et lui-même : $\boxed{n! + k \text{ n'est pas premier}}$. Les $n - 1$ entiers consécutifs $n! + 2$, …, $n! + n$ sont donc tous composés ; pour obtenir $L$ entiers consécutifs composés, il suffit de prendre $n = L + 1$. Par exemple, pour $n = 5$ : $122 = 2 \times 61$, $123 = 3 \times 41$, $124 = 4 \times 31$ et $125 = 5 \times 25$. Cela n'entre pas en contradiction avec la Proposition 3 : les nombres premiers sont en nombre infini, mais de plus en plus espacés « par endroits ».

2. On note $A_k = [\![k + 1; k + 10]\!]$. Cet ensemble contient 5 entiers pairs et 5 entiers impairs consécutifs $u$, $u + 2$, $u + 4$, $u + 6$, $u + 8$.

   - Le seul nombre premier pair est 2.
   - Parmi $u$, $u + 2$, $u + 4$, l'un est multiple de 3 : si $u = 3q$, c'est $u$ ; si $u = 3q + 1$, c'est $u + 2 = 3(q + 1)$ ; si $u = 3q + 2$, c'est $u + 4 = 3(q + 2)$. Ce multiple de 3 n'est premier que s'il vaut 3.

   Si $k \geqslant 3$, ni 2 ni 3 n'appartiennent à $A_k$ : au plus 4 des entiers impairs sont premiers, et aucun pair, donc $A_k$ contient au plus 4 nombres premiers. Il reste à examiner $k \in \{0 ; 1 ; 2\}$ : $A_0$ contient 2, 3, 5, 7 (quatre premiers), $A_1$ contient 2, 3, 5, 7, 11 (cinq premiers) et $A_2$ contient 3, 5, 7, 11 (quatre premiers). Le maximum vaut donc 5, atteint $\boxed{\text{uniquement pour } k = 1}$.




Les nombres premiers sont marqués en violet : la fenêtre $[\![2; 11]\!]$ est la seule à en contenir cinq, car elle contient à la fois 2 et 3, qui échappent aux arguments de parité et de divisibilité par 3, sans contenir 1, qui n'est pas premier.

## EXERCICE 37 ⋆⋆

1. Supposons que $\sqrt{3} = \frac{p}{q}$ avec $p$ et $q$ dans $\mathbb{N}^*$. Alors $p^2 = 3q^2$. Comparons l'exposant de 3 dans les décompositions en facteurs premiers des deux membres : si 3 apparaît avec l'exposant $a$ dans $p$ et $b$ dans $q$ (éventuellement nuls), il apparaît avec l'exposant $2a$, pair, dans $p^2$, et $2b + 1$, impair, dans $3q^2$. Cela contredit l'unicité de la décomposition. Ainsi $\boxed{\sqrt{3} \text{ est irrationnel}}$.
   **Généralisation :** si $n \in \mathbb{N}^*$ n'est pas le carré d'un entier, $\sqrt{n}$ est irrationnel. En effet, si tous les exposants $\alpha_i$ de la décomposition de $n$ étaient pairs, on aurait $n = \left(p_1^{\alpha_1/2} \cdots p_k^{\alpha_k/2}\right)^2$ ; l'un d'eux, $\alpha_i$, est donc impair. Si $\sqrt{n} = \frac{p}{q}$, alors $p^2 = nq^2$, et l'exposant de $p_i$ est pair à gauche et égal à $\alpha_i$ plus un nombre pair, donc impair, à droite : contradiction. Ainsi $\boxed{\sqrt{n} \in \mathbb{Q} \iff n \text{ est un carré parfait}}$.

2. Comme $6 = 2 \times 3$ n'est pas un carré (ses exposants sont impairs), $\boxed{\sqrt{6} \text{ est irrationnel}}$ d'après la question 1. Supposons que $r = \sqrt{2} + \sqrt{3}$ soit rationnel. Alors $r^2 = 2 + 2\sqrt{6} + 3$, donc $\sqrt{6} = \frac{r^2 - 5}{2}$ serait rationnel, ce qui est faux. Ainsi $\boxed{\sqrt{2} + \sqrt{3} \text{ est irrationnel}}$.

La preuve classique de l'irrationalité de $\sqrt{2}$, vue en Seconde, utilise une fraction irréductible ; celle-ci n'utilise que l'unicité de la décomposition, et s'adapte immédiatement à tout entier qui n'est pas un carré.

## EXERCICE 38 ⋆⋆⋆

Dans tout l'exercice, on décompose les entiers sur une même liste de nombres premiers $p_1$, …, $p_k$, quitte à autoriser des exposants nuls. D'après l'exercice 16, $\prod p_i^{\beta_i}$ divise $\prod p_i^{\alpha_i}$ si et seulement si $\beta_i \leqslant \alpha_i$ pour tout $i$.

1. Le sens direct est la question 6 de l'exercice 4. Réciproquement, si $a = \prod p_i^{\alpha_i}$ et $b = \prod p_i^{\beta_i}$, alors $a^2 = \prod p_i^{2\alpha_i}$ et $b^2 = \prod p_i^{2\beta_i}$. Si $a^2$ divise $b^2$, alors $2\alpha_i \leqslant 2\beta_i$, donc $\alpha_i \leqslant \beta_i$ pour tout $i$, et $a$ divise $b$. Ainsi $\boxed{a \mid b \iff a^2 \mid b^2}$.

2. Si $a = b = 1$, on prend $c = 1$. Sinon, avec $a = \prod p_i^{\alpha_i}$ et $b = \prod p_i^{\beta_i}$, l'égalité $a^2 = b^3$ et l'unicité de la décomposition donnent $2\alpha_i = 3\beta_i$ pour tout $i$. Ainsi 3 divise $2\alpha_i$ ; comme 3 est premier et ne divise pas 2, le lemme d'Euclide donne que 3 divise $\alpha_i$ : $\alpha_i = 3\gamma_i$, puis $3\beta_i = 6\gamma_i$, soit $\beta_i = 2\gamma_i$. En posant $c = \prod p_i^{\gamma_i}$, on obtient $\boxed{a = c^3 \text{ et } b = c^2}$. Par exemple, $8^2 = 4^3 = 64$ avec $c = 2$.

3. Pour $n = 1$, $d(1) = 1$ est impair et $1 = 1^2$. Pour $n \geqslant 2$, on a $d(n) = (\alpha_1 + 1)\cdots(\alpha_k + 1)$ avec des exposants $\alpha_i \geqslant 1$. Un produit d'entiers est impair si et seulement si chacun de ses facteurs est impair, donc $d(n)$ est impair si et seulement si tous les $\alpha_i$ sont pairs. Si c'est le cas, $n = \left(\prod p_i^{\alpha_i/2}\right)^2$ est un carré ; réciproquement, si $n = m^2$, les exposants de $n$ sont les doubles de ceux de $m$, donc pairs. Ainsi $\boxed{n \text{ est un carré } \iff d(n) \text{ est impair}}$.

On peut aussi le voir en associant chaque diviseur $d$ de $n$ au diviseur $\frac{n}{d}$ : les diviseurs vont par paires, sauf lorsque $d = \frac{n}{d}$, c'est-à-dire $d = \sqrt{n}$. Ainsi 36 a 9 diviseurs, son diviseur 6 étant « seul ».

## EXERCICE 39 ⋆⋆⋆

a) Soit $(m, n) \in E$ : $(m-1)(m+1) = 2^n$. On a $m \neq 1$, sinon $0 = 2^n$, donc $m \geqslant 2$ et $m - 1 \geqslant 1$. De plus $n \geqslant 1$, sinon $m^2 = 2$. Les entiers $m-1$ et $m+1$ sont des diviseurs positifs de $2^n$ ; d'après l'exercice 16, ils sont de la forme $2^k$ avec $0 \leqslant k \leqslant n$. Ainsi $\boxed{m - 1 = 2^a \text{ et } m + 1 = 2^b}$ avec $a < b$.

b) On a alors $2^b - 2^a = 2$. Si $a \geqslant 2$, le membre de gauche $2^a(2^{b-a} - 1)$ est divisible par 4, ce qui n'est pas le cas de 2. Si $a = 0$, on obtient $2^b = 3$, impossible. Il reste $a = 1$, qui donne $2^b = 4$, donc $m - 1 = 2$, soit $m = 3$, puis $2^n = 9 - 1 = 8$, soit $n = 3$. Réciproquement $(3, 3)$ convient, donc $\boxed{E = \{(3, 3)\}}$.

## EXERCICE 40 ⋆⋆⋆⋆

Pour $k \geqslant 1$, on note $N_k = 1 + 10^2 + 10^4 + \cdots + 10^{2k}$ l'entier qui s'écrit avec $k + 1$ chiffres 1 séparés par des 0 : $N_1 = 101$, $N_2 = 10101$, etc. D'après l'identité de l'exercice 30 a), appliquée à 100 et 1 :

$$99\, N_k = (100 - 1)(1 + 100 + \cdots + 100^k) = 100^{k+1} - 1 = \left(10^{k+1} - 1\right)\left(10^{k+1} + 1\right).$$

- **Si $k + 1 = 2j$ est pair**, alors $10^{k+1} - 1 = 100^j - 1$ est divisible par 99 (exercice 30 a)), et $N_k = \dfrac{100^j - 1}{99} \times \left(10^{k+1} + 1\right)$, où le premier facteur vaut $1 + 100 + \cdots + 100^{j-1}$. Pour $j = 1$, c'est-à-dire $k = 1$, on obtient $N_1 = 101$, qui est premier : il n'est divisible ni par 2, ni par 3, ni par 5, ni par 7, et $11^2 > 101$. Pour $j \geqslant 2$, les deux facteurs sont strictement supérieurs à 1, donc $N_k$ n'est pas premier.
- **Si $k+1$ est impair**, avec $k + 1 \geqslant 3$, alors 9 divise $10^{k+1} - 1$ (exercice 28) et $11 = 10 + 1$ divise $10^{k+1} + 1$ (exercice 30 b)). Ainsi :
$$N_k = \frac{10^{k+1} - 1}{9} \times \frac{10^{k+1} + 1}{11},$$
où le premier facteur est l'entier $11\ldots1$ à $k + 1$ chiffres, au moins égal à 111, et le second est au moins égal à $\frac{1001}{11} = 91$. Donc $N_k$ n'est pas premier.

Finalement, $\boxed{101 \text{ est le seul nombre premier de la liste}}$. *Vérification :* $10101 = 111 \times 91 = 3 \times 7 \times 13 \times 37$ et $1010101 = 101 \times 10001 = 73 \times 101 \times 137$.

## EXERCICE 41 : NOMBRES PARFAITS ⋆⋆⋆⋆

a) Les diviseurs de 6 autres que 6 sont 1, 2, 3, et $1 + 2 + 3 = 6$. Ceux de $28 = 2^2 \times 7$ sont 1, 2, 4, 7, 14, et $1 + 2 + 4 + 7 + 14 = 28$. Donc $\boxed{6 \text{ et } 28 \text{ sont parfaits}}$.

b) Comme $2^1 - 1 = 1$ n'est pas premier, on a $n \geqslant 2$, donc $p = 2^n - 1 \geqslant 3$ est un nombre premier impair, distinct de 2. La décomposition de $N$ est donc $N = 2^{n-1} \times p$, et d'après l'exercice 16, ses diviseurs sont les $2^i$ et les $2^i p$ pour $0 \leqslant i \leqslant n - 1$. Leur somme vaut :

$$(1 + 2 + \cdots + 2^{n-1})(1 + p) = (2^n - 1) \times 2^n = 2 \times 2^{n-1}(2^n - 1) = 2N,$$

en utilisant $1 + 2 + \cdots + 2^{n-1} = 2^n - 1$ (exercice 26, question 2). Ainsi $\boxed{N \text{ est parfait}}$.

Pour $n = 2$, 3, 5 et 7, on obtient les nombres parfaits 6, 28, 496 et 8128. Ce résultat figure déjà dans les Éléments d'Euclide (livre IX, proposition 36) ; Euler a démontré au XVIIIe siècle que tout nombre parfait pair est de cette forme. On ignore toujours s'il existe des nombres parfaits impairs.