# 15. Arithmétique, corrigé

**Exercice 1.** On cherche le reste modulo 10 de $17^{2022}$. On a $17 \equiv 7$ [10]. On a $7^2 \equiv -1$ [10]. On en déduit que $7^4 \equiv 1$ [10]. Ceci entraine que pour tout $n \in \mathbb{N}$, $7^{4n} \equiv 1$ [10]. Puisque $2023 = 4 \times 255 + 3$, on a $17^{2023} \equiv 1 \times 7^3 [10] \equiv 3$ [10]. On en déduit que le dernier chiffre de $17^{2023}$ est 9.

**Exercice 2.** On veut calculer $2222^3 \times 3^{2222}$ modulo 10.

Pour cela, on a $2222 \equiv 2$ [10] donc $2222^3 \equiv 8$ [10].

On a ensuite $3^2 \equiv -1$ [10]. On en déduit que $3^{2222} \equiv (-1)^{1111}$ [10] d'où $3^{2222} \equiv -1$ [10].

On en déduit finalement que $2222^3 \times 3^{2222} \equiv -8$ [10], ce qui entraine que le reste dans la division euclidienne par 10 vaut 2.

**Exercice 4.**

1) On a $10 \equiv -1$ [11]. Si on écrit $n$ sous la forme $n = \sum_{k=0}^{p} a_k 10^k$, alors, on a $n \equiv \sum_{k=0}^{p} (-1)^k a_k$ [11]. On en déduit que $n$ est divisible par 11 si et seulement si la somme de ses chiffres de rangs pairs moins la somme de ses chiffres de rangs impairs est divisible par 11.

**Exercice 5.** Soit $P(x) = 2x^3 - 3x^2 + 2x - 3$. Supposons que $P$ admette une racine entière $n_0$. On a alors $P(n_0) = 0$, c'est à dire que $n_0(2n_0^2 - 3n_0 + 2) = 3$.

On en déduit que $n_0$ divise 3. On a donc $n_0 = -3$, $n_0 = -1$, $n_0 = 1$ ou $n_0 = 3$. Or, on a $P(-3) = -90$, $P(-1) = -10$, $P(1) = -2$ et $P(3) = 30$. On en déduit que $P$ n'admet pas de racine entière.

**Exercice 6.**

1) En effectuant la table, on remarque que $2^3 \equiv 1$ [7] et que $3^6 \equiv 1$ [7].

2) Pour étudier les puissances de $3^n - 2^n$, on étudie donc selon les valeurs de $n$ modulo 6 :
   — Si $n \equiv 0$ [6], alors $3^n - 2^n \equiv 0$ [7].
   — Si $n \equiv 1$ [6], alors $3^n - 2^n \equiv 1$ [7].
   — Si $n \equiv 2$ [6], alors $3^n - 2^n \equiv 5$ [7].
   — Si $n \equiv 3$ [6], alors $3^n - 2^n \equiv 5$ [7].
   — Si $n \equiv 4$ [6], alors $3^n - 2^n \equiv 2$ [7].
   — Si $n \equiv 5$ [6], alors $3^n - 2^n \equiv 1$ [7].

**Exercice 12.** Pour $n \in \mathbb{N}$, on a $\sum_{k=0}^{n} 3^k = \frac{3^{n+1} - 1}{3 - 1} = \frac{3^{n+1} - 1}{2}$ par somme géométrique. On a donc 7 qui divise $\sum_{k=0}^{n} 3^k$ si et seulement si 14 divise $3^{n+1} - 1$.

Or, $14 = 2 \times 7$ et que $2 \wedge 7 = 1$, on a $14 | (3^{n+1} - 1)$ si et seulement si $2 | (3^{n+1} - 1)$ et $7 | (3^{n+1} - 1)$. Or, $3^{n+1} - 1$ est pair donc est toujours divisible par 2. Il reste à trouver les $n \in \mathbb{N}$ pour lesquels $7 | (3^{n+1} - 1)$, ce qui revient à avoir $3^{n+1} \equiv 1$ [7].

On a $3^2 \equiv 2\ [7]$, $3^3 \equiv 6\ [7]$, etc. , $3^6 \equiv 1\ [7]$ et 6 est la première puissance strictement positive vérifiant ceci. On en déduit que $3^n \equiv 1\ [7] \Leftrightarrow n \equiv 0\ [6]$.

Les entiers $n$ solutions sont donc les $n$ tels que $n+1 \equiv 0\ [6]$, soit les $n$ de la forme $6k+5$ avec $k \in \mathbb{N}$.

**Exercice 13.**

1) On a $n+3 = n+1+2$ donc $(n+1)|(n+3)$ si et seulement si $(n+1)|2$. Autrement dit, les seuls entiers $n$ qui conviennent sont $n=0$ et $n=1$.

On a de même $n^2+3n+5 = (n+2)(n+1)+3$. On a donc $(n+2)$ qui divise $n^2+3n+5$ si et seulement si $n+2$ divise 3. Puisque $n \in \mathbb{N}$, la seule solution est $n=1$.

**Exercice 14.** Soit $n \in \mathbb{Z}$. En utilisant le lemme d'Euclide, on trouve :

$$\begin{aligned}
(9n^2+10n+1) \wedge (9n^2+8n-1) &= (9n^2+10n+1-(9n^2+8n-1)) \wedge (9n^2+8n-1) \\
&= (2n+2) \wedge (9n^2+8n-1) \\
&= (2n+2) \wedge (9n^2+8n-1-(2n+2)\times 4n) \\
&= (2n+2) \wedge (n^2-1) \\
&= (2(n+1)) \wedge ((n-1)(n+1)) \\
&= |n+1| \times (2 \wedge (n-1)).
\end{aligned}$$

On en déduit que le PGCD étudié vaut $2|n+1|$ si $n$ est impair et $|n+1|$ si $n$ est pair. *Attention aux valeurs absolues ! Un PGCD est toujours positif !*

**Exercice 15.** Soient $(x,y) \in (\mathbb{N}^*)^2$. On a :

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{5} \Leftrightarrow 5y+5x = xy \Leftrightarrow 5y = x(y-5).$$

Autrement dit, on a $y \neq 5$ et $x = \dfrac{5y}{y-5} \in \mathbb{N}^*$. Or, on a :

$$5y = 5(y-5)+25.$$

On a donc $y-5$ qui divise $5y$ si et seulement si $y-5$ divise 25. Or, les diviseurs de 25 sont $-25, -5, -1, 1, 5, 25$. On en déduit que les possibilités pour $y$ (puisque $y \in \mathbb{N}^*$) sont $4, 6, 10, 30$. Si $y=4$, on a $x<0$ donc on enlève cette solution. Pour les autres valeurs, on a $x \in \mathbb{N}^*$ donc finalement les solutions sont les couples $(x,y)$ de la forme $(30,6), (10,10), (6,30)$.

**Exercice 16.** Résoudre dans $\mathbb{Z}$ les équations suivantes :

1) Calculons le pgcd de 151 et 77 en utilisant l'algorithme d'Euclide. On a :

$$\begin{aligned}
151 &= 77+74 \\
77 &= 74+3 \\
74 &= 24\times 3+2 \\
3 &= 2+1
\end{aligned}$$

On en déduit que $151 \wedge 77 = 1$. Ceci entraine que l'équation $151x-77y=5$ admet une infinité de solutions que l'on va déterminer. Commençons pour trouver une solution particulière en remontant l'algorithme d'Euclide. On a :

$$\begin{aligned} 1 &= 3-2 \\ &= 3-(74-24\times 3) \\ &= 25\times 3-74 \\ &= 25\times(77-74)-74 \\ &= 25\times 77-74\times 26 \\ &= 25\times 77-(151-77)\times 26 \\ &= 51\times 77-26\times 151. \end{aligned}$$

Pour obtenir une solution particulière, il faut multiplier par 5 les nombres trouvés. On en déduit que le couple $(x_0, y_0$ avec $x_0 = -130$ et $y_0 = -255$ est une solution particulière de $(E)$. Désterminons alors par analyse/synthèse l'ensemble des solutions.

**Analyse :** soit $(x, y)$ solution de l'équation considérée. On a a alors $151x - 77y = 151x_0 - 77y_0$. On en déduit que :

$$151(x - x_0) = 77(y - y_0).$$

Ceci entraine que 151 divise $77(y - y_0)$. Or, $151 \wedge 77 = 1$. D'après le théorème de Gauss, on a donc 151 qui divise $y - y_0$. Il existe donc $k \in \mathbb{Z}$ tel que $y - y_0 = 151k$. En réinjectant dans la relation précédente et en simplifiant par 151, on trouve alors que $x - x_0 = 77k$. On en déduit que $x = x_0 + 77k$ et $y = y_0 + 151k$ avec $k \in \mathbb{Z}$.

**Synthèse :** Réciproquement, supposons que $x = x_0 + 77k$ et $y = y_0 + 151k$ avec $k \in \mathbb{Z}$. On a alors :

$$\begin{aligned} 151x - 77y &= 151(x_0 + 77k) - 77(y_0 + 151k) \\ &= 151x_0 - 77y_0 + 0 \\ &= 5. \end{aligned}$$

La dernière égalité étant vraie puisque $(x_0, y_0$ est solution particulière. On a donc montré par analyse/synthèse que l'ensemble des solutions de l'équation est l'ensemble :

$$\{(-130 + 77k, -255 + 151k),\ k \in \mathbb{Z}\}.$$

2) Calculons le pgcd de 51 et 44. On a :

$$\begin{aligned} 51 &= 44 + 7 \\ 44 &= 6\times 7 + 2 \\ 7 &= 3\times 2 + 1. \end{aligned}$$

On en déduit que $51 \wedge 44 = 1$. L'équation $51x + 44y = 1$ admet donc une infinité de solutions. Pour en trouver une particulière, on remonte l'algorithme d'Euclide :

$$\begin{aligned} 1 &= 7 - 3\times 2 \\ &= 7 - 3\times(44 - 6\times 7) \\ &= 19\times 7 - 3\times 44 \\ &= 19\times(51 - 44) - 3\times 44 \\ &= 19\times 51 - 22\times 44. \end{aligned}$$

On en déduit qu'une solution particulière de $51x + 44y = 1$ est $(x_0, y_0)$ avec $x_0 = 19$ et $y_0 = -22$. Ceci entraine (même preuve que dans le cours ou dans le 1.) que l'ensemble des solutions est :

$$\{(19 + 44k, -22 - 51k),\ k \in \mathbb{Z}\}.$$

3) On remarque déjà que dans l'équation $9072x + 306y = 18$, les nombres 9072 et 306 sont divisibles par 6 (car ils sont pairs et leur somme des chiffres vaut 3). L'équation est donc équivalente à $1512x + 51y = 3$. On peut encore simplifier par 3 encore une fois (même argument). L'équation est donc équivalente à $504x + 17y = 1$. On effectue alors la division euclidienne de 504 par 17 :

$$\begin{aligned} 504 &= 29 \times 17 + 11 \\ 17 &= 11 + 6 \\ 11 &= 6 + 5 \\ 6 &= 5 + 1. \end{aligned}$$

On en déduit que $504 \wedge 17 = 1$. L'équation admet donc une infinité de solutions. En remontant l'algorithme d'Euclide, on trouve une solution particulière. On a :

$$\begin{aligned} 1 &= 6 - 5 \\ &= 6 - (11 - 6) \\ &= 2 \times 6 - 11 \\ &= 2 \times (17 - 11) - 11 \\ &= 2 \times 17 - 3 \times 11 \\ &= 2 \times 17 - 3 \times (504 - 29 \times 17) \\ &= -3 \times 504 + 89 \times 17. \end{aligned}$$

On trouve alors une solution particulière de $504x + 17y = 1$. Par exemple, $(x_0, y_0)$ avec $x_0 = -6$ et $y_0 = 178$ convient. On a alors (voir cours ou 1.) que l'ensemble des solutions de l'équation est :

$$\{(-6 + 17k, 178 - 504k),\ k \in \mathbb{Z}\}.$$

**Exercice 17.** (i) Soient $a, b \in \mathbb{Z}$.

Supposons dans un premier temps que $a \wedge b = 1$. D'après le lemme d'Euclide, on a $a \wedge (a + b) = a \wedge (a + b - a) = a \wedge b = 1$. De mÃªme, on a aussi $b \wedge (a + b) = 1$. On en déduit d'après le cours que :

$$(ab) \wedge (a + b) = 1.$$

Réciproquement, supposons que $(ab) \wedge (a + b) = 1$. D'après l'identité de Bézout, il existe alors $u, v \in \mathbb{Z}$ tels que $abu + (a + b)v = 1$, ce qui implique que :

$$a(bu + v) + bv = 1.$$

D'après le théorème de Bézout, on en déduit que $a \wedge b = 1$ (puisque $bu + v \in \mathbb{Z}$ et $v \in \mathbb{Z}$).

**Exercice 19.** Soit $x \in \mathbb{Q}$. On suppose qu'il existe $n \in \mathbb{N}^*$ tel que $x^n \in \mathbb{Z}$. Puisque $x \in \mathbb{Q}$, on peut écrire $x = \dfrac{p}{q}$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et $p \wedge q = 1$. On a alors :

$$x^n = \frac{p^n}{q^n}.$$

On a alors $p^n \wedge q^n = 1$ puisque $p \wedge q = 1$ (on peut par exemple utiliser le fait que $p$ et $q$ n'ont aucun facteur premier commun donc c'est aussi le cas de $p^n$ et $q^n$).

Puisque $x^n \in \mathbb{Z}$, on en déduit qu'il existe $k \in \mathbb{Z}$ tel que $\dfrac{p^n}{q^n} = k = \dfrac{k}{1}$. Or, on a unicité de l'écriture sous la forme $\dfrac{p}{q}$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et $p \wedge q = 1$, on en déduit que $p^n = k$ et $q^n = 1$. Puisque $q \in \mathbb{N}^*$, on a alors $q = 1$ et donc $x = p \in \mathbb{Z}$.

**Exercice 21.**

1) Notons $(E)$ : $x \wedge y = x + y - 1$.

**Analyse :** Supposons que $(x, y)$ soit solution de $(E)$. Supposons dans un premier temps que $x \wedge y \neq 1$. Posons alors $a = x \wedge y$. Puisque $a|x$ et $a|y$, on en déduit que $a| - 1$. On a donc $a = 1$ (car $a$ est positif). Ceci est donc absurde !

On a donc $x \wedge y = 1$. L'équation $(E)$ est donc équivalente à :

$$\begin{cases} x + y = 2 \\ x \wedge y = 1 \end{cases}$$

On en déduit que $(x, y) \in \{(n, 2-n),\ n \in \mathbb{Z}\}$ et que $x \wedge y = 1$. Déterminons quels sont les éléments de cet ensemble premiers entre eux. On a :

$$\begin{array}{rcll} n \wedge (2-n) & = & n \wedge (2-n+n) & \text{(d'après le lemme d'Euclide)} \\ & = & n \wedge 2. & \end{array}$$

On en déduit que ce pgcd vaut 1 si et seulement si $n$ est impair. On trouve donc que $(x, y)$ est de la forme $(2k+1, 1-2k)$, avec $k \in \mathbb{Z}$.

**Synthèse :** Soit $k \in \mathbb{Z}$. On a alors $(2k+1) \wedge (1-2k) = 1$ (toujours en utilisant le lemme d'Euclide) et en remarquant que $(2k+1) \wedge 2 = 1$. On a alors que $2k + 1 + (1-2k) - 1 = (2k+1) \wedge (1-2k)$. Tous les couples trouvés sont donc solutions.

L'ensemble des solutions de $(E)$ est donc l'ensemble $\{(2k+1, 1-2k),\ k \in \mathbb{Z}\}$.

2) Notons $(E')$ : $x \vee y = x + y - 1$.

**Analyse :** Supposons $(x, y)$ solution de $(E')$. Supposons dans un premier temps que $x \wedge y \neq 1$. Posons alors $a = x \wedge y$. Puisque $a | x \vee y$, $a | x$ et $a | y$, on en déduit que $a | -1$. On a donc $a = 1$ (car $a$ est positif). Ceci est donc absurde !

On a donc $x \wedge y = 1$, ce qui implique que $x \vee y = xy$. L'équation $(E')$ est donc équivalente à :

$$\begin{cases} xy = x + y - 1 \\ x \wedge y = 1 \end{cases}$$

On en déduit que $y(x-1) = x - 1$, ce qui après factorisation entraîne que $(x-1)(y-1) = 0$. On en déduit que $(x, y) \in \{(k, 1),\ k \in \mathbb{Z}\} \bigcup \{(1, j) n\ j \in \mathbb{Z}\}$.

**Synthèse :** Soit $k \in \mathbb{Z}$. On a alors $k \vee 1 = k$. et on a alors que $k = k + 1 - 1$. $(k, 0)$ est donc solution de $(E')$. De même, $(1, k)$ est solution de $(E')$. Tous les couples trouvés sont donc solutions.

L'ensemble des solutions de $(E)$ est donc l'ensemble $\{(k, 1),\ k \in \mathbb{Z}\} \bigcup \{(1, j),\ j \in \mathbb{Z}\}$.

**Exercice 22.** On considère $(E)$ : $3^x = 8 + y^2$ avec $x, y \in \mathbb{N}^*$. Soit $(x, y)$ une solution de $(E)$.

1) $3^x$ est impair (un produit de nombre impair est impair) donc $y^2 = 3^x - 8$ est impair. On en déduit que $y$ est impair (par l'absurde, si il était pair alors $y^2$ serait pair : absurde).

Étudions alors les restes possibles des carrés modulo 8 pour $n \in \mathbb{Z}$ (impair car on a montré que $y$ était impair) :

$$\begin{cases} n \equiv 1\ [8] \Rightarrow n^2 \equiv 1\ [8] \\ n \equiv 3\ [8] \Rightarrow n^2 \equiv 1\ [8] \\ n \equiv 5\ [8] \Rightarrow n^2 \equiv 1\ [8] \\ n \equiv 7\ [8] \Rightarrow n^2 \equiv 1\ [8] \end{cases}$$

Tous les carrés impairs sont congrus à 1 modulo 8. On en déduit que $y^2 \equiv 1[8]$.

2) On déduit de la question précédente que $3^x \equiv 1\ [8]$. Supposons par l'absurde que $x$ soit impair, c'est à dire de la forme $x = 2k + 1$ avec $k \in \mathbb{N}$. On en déduit que $3^x \equiv 3\ [8]$ ce qui est absurde !

On en déduit que $x$ est pair, donc de la forme $2k$ avec $k \in \mathbb{N}^*$. On en déduit alors que $3^{2k} - y^2 = 8$, ce qui implique que :

$$(3^k - y)(3^k + y) = 8.$$

Or, puisque $y$ est supposé positif, on en déduit que $3^k - y \geq 1$ (sinon on aurait le produit d'un nombre inférieur ou égal à 0 avec un nombre positif qui serait égal à 8, ce qui est absurde). On en déduit que $3^k + y \leq 8$. Puisque $y > 0$, ceci implique que $3^k < 8$, c'est à dire $3^{\frac{x}{2}} < 8$.

3) L'unique valeur possible pour $x$ est donc 2. Ceci impose $y = 1$. L'unique solution de notre système est donc $x = 2$ et $y = 1$.

**Exercice 23.** Supposons par l'absurde que l'équation $(E)$ : $x^2 + y^2 = 11z^2$ admette une solution entière. Posons $a = x \wedge y \wedge z$. On remarque alors que si l'on pose $x' = \frac{x}{a}$, $y' = \frac{y}{a}$ et $z' = \frac{z}{a}$, alors, $x', y'$ et $z'$ sont encore entiers, ils sont premiers entre eux dans leur ensemble et ils sont encore solution de $(E)$ (en divisant l'équation par $a^2$.

Considérons alors l'équation modulo 11. On a donc $(x')^2 + (y')^2 \equiv 0$ [11]. Étudions à présent les restes possibles pour les carrés modulo 11. Si $n \in \mathbb{Z}$, alors :

$$\begin{cases} n \equiv 0 \ [11] \Rightarrow n^2 \equiv 0 \ [11] \\ n \equiv 1 \ [11] \Rightarrow n^2 \equiv 1 \ [11] \\ n \equiv 2 \ [11] \Rightarrow n^2 \equiv 4 \ [11] \\ n \equiv 3 \ [11] \Rightarrow n^2 \equiv 9 \ [11] \\ n \equiv 4 \ [11] \Rightarrow n^2 \equiv 5 \ [11] \\ n \equiv 5 \ [11] \Rightarrow n^2 \equiv 3 \ [11] \\ n \equiv 6 \ [11] \Rightarrow n^2 \equiv 3 \ [11] \\ n \equiv 7 \ [11] \Rightarrow n^2 \equiv 5 \ [11] \\ n \equiv 8 \ [11] \Rightarrow n^2 \equiv 9 \ [11] \\ n \equiv 9 \ [11] \Rightarrow n^2 \equiv 4 \ [11] \\ n \equiv 10 \ [11] \Rightarrow n^2 \equiv 1 \ [11] \end{cases}$$

Pour que $x^2 + y^2 \equiv 0$ [11], alors, on doit avoir $x \equiv 0$ [11] et $y \equiv 0$ [11] (on ne peut pas retomber sur 0 avec les différents restes ci-dessus dans tous les autres cas). On en déduit donc que $11|x'$ et que $11|y'$. On a donc $11^2|(x')^2$ et $11^2|(y')^2$. Puisque $(x', y', z')$ vérifie l'équation $(E)$, on en déduit que $11^2$ divise $(x')^2 + (y')^2 = 11(z')^2$, ce qui implique que $11|(z')^2$. Puisque 11 est premier, on en déduit que $11|z'$ (on a $11|(z') \times (z')$ ssi $11|z'$ ou $11|z'$). On en déduit que $x'$, $y'$ et $z'$ ne sont pas premiers entre eux dans leur ensemble ce qui est absurde !

L'équation proposée n'a donc pas de solution.

**Exercice 24.** Supposons par l'absurde que $x, y, z) \in \mathbb{Z}^3$ soit solution de $x^3 + y^3 + z^3 = 94$. On a alors que $x^3 + y^3 + z^3 \equiv 4$ [9]. Calculons les restes possibles de $n^3$ modulo 9 pour $n \in \mathbb{Z}$ :

$$\begin{cases} n \equiv 0 \ [9] \Rightarrow n^3 \equiv 0 \ [9] \\ n \equiv 1 \ [9] \Rightarrow n^3 \equiv 1 \ [9] \\ n \equiv 2 \ [9] \Rightarrow n^3 \equiv -1 \ [9] \\ n \equiv 3 \ [9] \Rightarrow n^3 \equiv 0 \ [9] \\ n \equiv 4 \ [9] \Rightarrow n^3 \equiv 1 \ [9] \\ n \equiv 5 \ [9] \Rightarrow n^3 \equiv -1 \ [9] \\ n \equiv 6 \ [9] \Rightarrow n^3 \equiv 0 \ [9] \\ n \equiv 7 \ [9] \Rightarrow n^3 \equiv 1 \ [9] \\ n \equiv 8 \ [9] \Rightarrow n^3 \equiv -1 \ [9] \end{cases}$$

Les restes possibles des cubes modulo 9 sont donc 0,1 et -1. En prenant des combinaisons de ces restes, on peut donc obtenir les restes 0,1,2,3,-1,-2,-3 mais on ne peut pas obtenir 4. L'équation étudiée n'a donc pas de solutions entières.

**Exercice 26.** Soient $p_1, \ldots, p_n$ des nombres premiers distincts. On pose $A = \sum_{k=1}^{n} \frac{1}{p_k}$. Supposons par l'absurde que $A$ soit entier. On peut alors multiplier $A$ par $\prod_{j=1}^{n} p_j$, ce qui nous donne :

$$A \prod_{j=1}^{n} p_j = \sum_{k=1}^{n} \prod_{j \neq k} p_j.$$

Or, $p_1$ divise le membre de gauche donc il divise également la somme de droite. Or, $p_1$ apparait dans chacun des produits sauf dans le terme $\prod_{j \neq 1} p_j$. Ceci entraine que $p_1 | \prod_{j \neq 1} p_j$. Or, ceci est absurde car $p_1$ est premier avec tous les $p_j$ (car ce sont des nombres premiers distincts) et est donc premier avec $\prod_{j \neq 1} p_j$. Il ne peut donc pas le diviser.

**Exercice 28.** Soit $n$ dans $\mathbb{N}^*$. Posons $x = (n+1)! + 1$. $x+1$ n'est pas premier car il est divisible par 2. $x+2$ n'est pas premier car il est divisible par 3. De manière générale, si $k \in [\![1, n]\!]$, alors $x+k$ est divisible par $k+1$. On a donc construit $n$ entiers consécutifs non premiers.

**Exercice 29.** Soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ la décomposition en facteur premier de $n \in \mathbb{N}^*$.

1) Les diviseurs de $n$ sont de la forme $\prod_{i=1}^{k} p_i^{\beta_i}$ où pour tout $i \in [\![1, k]\!]$, $0 \leq \beta_i \leq \alpha_i$. On a donc $\alpha_1 + 1$ possibilités pour le choix de la puissance de $p_1$, puis $\alpha_2 + 1$ possibilités pour le choix de la puissance de $p_2$, etc., et enfin $\alpha_k + 1$ possibilités pour le choix de la puissance de $p_k$. On en déduit qu'il existe finalement $\prod_{i=1}^{k} (\alpha_i + 1)$ possibilités pour construire un diviseur positif de $n$, ce qui nous donne le nombre de diviseurs positifs distincts.

2) On veut $\prod_{i=1}^{k} (\alpha_i + 1) = 21 = 7 \times 3$. On ne peut donc avoir qu'au plus deux $\alpha_i$ strictement positif (sinon on aurait un nombre admettant plus de facteurs premiers). On a donc plusieurs possibilités pour obtenir 21 :

- Soit $k = 1$ et $\alpha_1 = 20$. Le plus petit nombre de cette forme est $2^{20}$.
- Soit $k = 2$ et $\alpha_1 = 2$ et $\alpha_2 = 6$. Le plus petit nombre de cette forme est $2^6 \times 3^2$.

Le plus petit entier admettant 21 diviseurs positifs est donc $2^6 \times 3^2 = 576$.

**Exercice 30.**

1) On doit ici montrer que $n^5 - n$ est divisible par $30 = 2 \times 3 \times 5$. Puisque ces 3 entiers sont premiers entre eux, on va tester la divisilité par 2, par 3 et par 5 et le corollaire du théorème de Gauss nous assure alors que le produit de ces 3 entiers divisera $n^5 - n$. Commençons par la divisibilité par 5 : d'après le petit théorème de Fermat, $n^5 \equiv n$ [5], ce qui nous donne que $n^5 - n$ est divisible par 5. Pour les autres divisibilités, on peut essayer de factoriser :

$$\begin{aligned} n^5 - n &= n(n^4 - 1) \\ &= n(n^2 - 1)(n^2 + 1) \\ &= n(n-1)(n+1)(n^2+1). \end{aligned}$$

On a alors le produit de 3 entiers consécutifs dans l'expression de $n^5 - n$, ce qui entraine que 6 divise $n^5 - n$ (car 2 le divise et 3 le divise et 2 et 3 sont premiers entre eux). Puisque 5 et 6 sont premiers

entre eux, on en déduit que 30 divise $n^5 - n$. *On pourrait aussi réutiliser le théorème de Fermat pour montrer la divisibilité par 2 et par 3, voir la question suivante.*

2) On a directement avec Fermat $n^7 \equiv n$ [7], c'est à dire que 7 divise $n^7 - n$. Il ne reste plus qu'à montrer que 6 divise $n^7 - n$ (car 6 et 7 sont premiers entre eux). On pourrait le faire comme ci-dessus mais on peut également le faire en réutilisant Fermat. En effet, on a $n^3 \equiv n$ [3] (d'après Fermat) donc on en déduit que :

$$\begin{aligned} n^7 &\equiv n^3 \times n^4 \ [3] \\ &\equiv n \times n^4 \ [3] \\ &\equiv n^3 \times n^2 \ [3] \\ &\equiv n \times n^2 \ [3] \\ &\equiv n \ [3]. \end{aligned}$$

Ceci entraine que 3 divise $n^7 - n$. De même, puisque $n^2 \equiv n$ [2]. On en déduit que :

$$\begin{aligned} n^7 &\equiv (n^2)^3 \times n \ [2] \\ &\equiv n^4 \ [2] \\ &\equiv (n^2)^2 \ [2] \\ &\equiv n^2 \ [2] \\ &\equiv n \ [2]. \end{aligned}$$

On a donc 2 qui divise $n^7 - n$. Puisque 2, 3 et 7 sont premiers entre eux, on en déduit que 42 divise $n^7 - n$. Montrer que $n^7 - n$ est divisible par 42.

**Exercice 31. Infinité de nombres premiers de la forme $4k + 3$.**

1) Soit $n \equiv 3$ [4]. On a alors $n$ impair (car $n$ est de la forme $4k + 3$). On en déduit que les nombres premiers qui sont dans la décomposition en facteurs premiers de $n$ sont tous impairs. Ces nombres sont donc tous congrus à 1 ou 3 modulo 4.

Supposons par l'absurde que tous ces nombres soient congrus à 1 modulo 4. Alors, par produit, on aurait $n$ qui serait congru à $1 \times 1 \times \ldots \times 1$ [4] ce qui est absurde car $n$ est congru à 3 modulo 4.

On en déduit que $n$ admet au moins un diviseur premier congru à 3 modulo 4.

2) Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombre premiers de la forme $4n + 3$. Notons les $p_1, \ldots, p_k$. Par hypothèse, ce sont les seuls nombres premiers qui sont congrus à 3 modulo 4. Remarquons qu'ils sont tous impairs (2 n'étant pas congru à 3 modulo 4).

Considérons alors le nombre $x = 2\prod_{j=1}^{k} p_j + 1$. Puisque chaque $p_j$ est congruent à 3 modulo 4, on en déduit que le produit $\prod_{j=1}^{k} p_j$ est congruent à 1 ou 3 (puisqu'il s'agit d'un nombre impair). En multipliant par 2, on obtient un nombre congru à 2 modulo 4 ou à 6 modulo 4, ce qui dans les deux cas, revient à avoir un nombre congru à 2 modulo 4. On a donc $x \equiv 3$ [4].

D'après la question précédente, on a $x$ qui admet un diviseur premier congru à 3 modulo 4. Or, aucun des $p_j$ ne divise $x$ (puisqu'ils divisent le produit, si $p_j$ divise $x$, alors $p_j$ divise 1 ce qui est absurde). Ceci contredit le fait qu'il n'y a que $p_1, \ldots, p_k$ qui soient premiers congrus à 3 modulo 4.

On en déduit qu'il y a une infinité de nombres premiers de la forme $4n + 3$.

**Exercice 32. Infinité de nombres premiers de la forme $4k + 1$.**

1) On a $n^p \equiv n\ [p]$ d'après le petit théorème de Fermat donc $p|(n^p - n)$, soit $p|n(n^{p-1} - 1)$. Puisque $p \wedge n = 1$, on en déduit d'après le théorème de Gauss que $p|(n^{p-1} - 1)$, soit que $n^{p-1} \equiv 1\ [p]$.

2) Soit $n \in \mathbb{N}$ et $p \in \mathbb{P}$ un nombre premier impair tel que $p$ divise $n^2 + 1$. On a $p$ qui ne divise pas $n$ (car sinon $p$ divise $n^2$ et donc $p$ divise $(n^2 + 1) - n^2 = 1$ ce qui est absurde car $p \geq 2$). Puisque $p$ est premier, on a $n \wedge p = 1$.

D'après la question précédente, on a alors $n^{p-1} \equiv 1\ [p]$. Or, on a $p|(n^2 + 1)$ donc $n^2 \equiv -1\ [p]$. En élevant à la puissance $\dfrac{p-1}{2} \in \mathbb{N}^*$ (puisque $p$ est impair), on a alors que :

$$n^{2\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}\ [p] \Leftrightarrow n^{p-1} \equiv (-1)^{\frac{p-1}{2}}\ [p].$$

On a donc $(-1)^{\frac{p-1}{2}} \equiv 1\ [p]$ ce qui entraine que $\dfrac{p-1}{2}$ est pair (sinon on aurait $1 \equiv -1\ [p]$ ce qui est absurde car $p > 2$). On a donc $p - 1$ multiple de 4, soit $p \equiv 1\ [4]$.

3) Supposons par l'absurde qu'il n'y ait qu'un nombre fini de nombres premiers congrus à 1 modulo 4. Notons les $p_1, \ldots, p_k$. Considérons alors $a = (2p_1 \times p_2 \times \ldots \times p_n)^2 + 1$. Soit $p \in \mathbb{P}$ qui divise $a$. Puisque $a$ est impair, on a $p$ impair. D'après la question précédente, on a donc $p \equiv 1\ [4]$. Il existe donc $j \in [\![1, k]\!]$ tel que $p = p_j$. Ceci est absurde car on a alors $p_j$ qui divise $a$ et qui divise $(2p_1 \times p_2 \times \ldots \times p_n)^2$ (car il apparait dans le produit) et il divise donc la différence, soit 1.

On a donc une infinité de nombres premiers congrus à 1 modulo 4.