



Arithmétique

Exercices de Jean-Louis Rouget. Retrouver aussi cette fiche sur www.maths-france.fr

* très facile ** facile *** difficulté moyenne **** difficile ***** très difficile

I : Incontournable T : pour travailler et mémoriser le cours

Exercice 1 **

Montrer que le produit de quatre entiers consécutifs, augmenté de 1, est un carré parfait.

[Correction ▼](#)

[005291]

Exercice 2 ***T

1. Montrer que $\forall n \in \mathbb{Z}, 6 \mid 5n^3 + n$.
2. Montrer que $\forall n \in \mathbb{N}, 7 \mid 4^{2^n} + 2^{2^n} + 1$.

[Correction ▼](#)

[005292]

Exercice 3 ***IT

Un entier de la forme $8n + 7$ ne peut pas être la somme de trois carrés parfaits.

[Correction ▼](#)

[005293]

Exercice 4 **IT

Pour $n \in \mathbb{N}^*$, on pose $(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}$ où $(a_n, b_n) \in (\mathbb{N}^*)^2$. Montrer que $a_n \wedge b_n = 1$.

[Correction ▼](#)

[005294]

Exercice 5 ****

Montrer que, pour tout entier naturel n , 2^{n+1} divise $E((1 + \sqrt{3})^{2n+1})$.

[Correction ▼](#)

[005295]

Exercice 6 ***IT

Soient A la somme des chiffres de 4444^{4444} et B la somme des chiffres de A . Trouver la somme des chiffres de B . (Commencer par majorer la somme des chiffres de $n = a_0 + 10a_1 + \dots + 10^p a_p$.)

[Correction ▼](#)

[005296]

Exercice 7 **

Montrer que si p est premier et $8p^2 + 1$ est premier alors $8p^2 - 1$ est premier.

[Correction ▼](#)

[005297]

Exercice 8 **I

1. Montrer que $\forall (k, n) \in (\mathbb{N}^*)^2, [k \wedge n = 1 \Rightarrow n \mid C_n^k]$.
2. Montrer que $\forall n \in \mathbb{N}^*, (n+1) \mid C_{2n}^n$.

[Correction ▼](#)

[005298]

Exercice 9 **T

Résoudre dans $(\mathbb{N}^*)^2$ les équations ou systèmes d'équations suivants :

$$1) \begin{cases} x+y=56 \\ x \vee y=105 \end{cases} \quad 2) \begin{cases} x \wedge y=x-y \\ x \vee y=72 \end{cases} \quad 3) x \vee y - x \wedge y = 243.$$

[Correction ▼](#)

[005299]

Exercice 10 ***

Montrer que la somme de cinq carrés parfaits d'entiers consécutifs n'est jamais un carré parfait.

[Correction ▼](#)

[005300]

Exercice 11 ***IT

Pour $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$ (nombres de FERMAT). Montrer que les nombres de Fermat sont deux à deux premiers entre eux.

[Correction ▼](#)

[005301]

Exercice 12 ***

Soit $(u_n)_{n \in \mathbb{N}}$ la suite définie par $u_0 = 0$, $u_1 = 1$ et $\forall n \in \mathbb{N}$, $u_{n+2} = u_{n+1} + u_n$ (suite de FIBONACCI).

1. Montrer que $\forall n \in \mathbb{N}^*$, $u_{n+1}u_{n-1} - u_n^2 = (-1)^n$ et en déduire que $\forall n \in \mathbb{N}^*$, $u_n \wedge u_{n+1} = 1$.
2. Montrer que $\forall n \in \mathbb{N}$, $\forall m \in \mathbb{N}^*$, $u_{m+n} = u_m u_{n+1} + u_{m-1} u_n$ et en déduire que $u_m \wedge u_n = u_{m \wedge n}$ pour m et n non nuls.

[Correction ▼](#)

[005302]

Exercice 13 ***I

On veut résoudre dans \mathbb{Z}^3 l'équation $x^2 + y^2 = z^2$ (de tels triplets d'entiers relatifs sont appelés triplets pythagoriciens, comme par exemple $(3, 4, 5)$).

1. Montrer que l'on peut se ramener au cas où $x \wedge y \wedge z = 1$. Montrer alors que dans ce cas, x , y et z sont de plus deux à deux premiers entre eux.
2. On suppose que x , y et z sont deux à deux premiers entre eux. Montrer que deux des trois nombres x , y et z sont impairs le troisième étant pair puis que z est impair.

On suppose dorénavant que x et z sont impairs et y est pair. On pose $y = 2y'$, $X = \frac{z+x}{2}$ et $Z = \frac{z-x}{2}$.

3. Montrer que $X \wedge Z = 1$ et que X et Z sont des carrés parfaits.
4. En déduire que l'ensemble des triplets pythagoriciens est l'ensemble des triplets de la forme

$$(d(u^2 - v^2), 2d uv, d(u^2 + v^2))$$

où $d \in \mathbb{N}$, $(u, v) \in \mathbb{Z}^2$, à une permutation près des deux premières composantes.

[Correction ▼](#)

[005303]

Exercice 14 **

Résoudre dans \mathbb{N}^2 l'équation $3x^3 + xy + 4y^3 = 349$.

[Correction ▼](#)

[005304]

Exercice 15 ***

Résoudre dans $(\mathbb{N}^*)^2$ l'équation d'inconnue $(x, y) : \sum_{k=1}^x k! = y^2$.

[Correction ▼](#)

[005305]

Exercice 16 ***

Montrer que $n = 4...48...89$ (p chiffres 4 et $p-1$ chiffres 8 et donc $2p$ chiffres) (en base 10) est un carré parfait.

[Correction ▼](#)

[005306]

Exercice 17 *I**

Montrer que tout nombre impair non divisible par 5 admet un multiple qui ne s'écrit (en base 10) qu'avec des 1 (par exemple, $37.1 = 37$, $37.2 = 74$, $37.3 = 111$).

[Correction ▼](#)

[005307]

Exercice 18 ***

Soit $u_n = 10...01_2$ (n chiffres égaux à 0). Déterminer l'écriture binaire de :

1. u_n^2 ,
2. u_n^3 ,
3. $u_n^3 - u_n^2 + u_n$.

[Correction ▼](#)

[005308]

Exercice 19 **I

1. Déterminer en fonction de n entier non nul, le nombre de chiffres de n en base 10.
2. Soit $\sigma(n)$ la somme des chiffres de n en base 10.
 - (a) Montrer que la suite $\left(\frac{\sigma(n+1)}{\sigma(n)}\right)_{n \geq 1}$ est bornée. Cette suite converge-t-elle ?
 - (b) Montrer que pour tout naturel non nul n , $1 \leq \sigma(n) \leq 9(1 + \log n)$.
 - (c) Montrer que la suite $(\sqrt[n]{\sigma(n)})_{n \geq 1}$ converge et préciser sa limite.

[Correction ▼](#)

[005309]

Exercice 20 *I**

1. (Formule de LEGENDRE) Soit n un entier naturel supérieur ou égal à 2 et p un nombre premier. Etablir que l'exposant de p dans la décomposition de $n!$ en facteurs premiers est

$$E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + E\left(\frac{n}{p^3}\right) + \dots$$

2. Par combien de 0 se termine l'écriture en base 10 de $1000!$?

[Correction ▼](#)

[005310]

Exercice 21 *I Petit théorème de FERMAT**

Soit p un nombre premier.

1. Montrer que, pour tout entier k tel que $1 \leq k \leq p-1$, p divise C_p^k .
2. Montrer que $\forall a \in \mathbb{N}^*$, $a^p \equiv a \pmod{p}$ (par récurrence sur a).

[Correction ▼](#)

[005311]

Exercice 22 *I Théorème de WILSON**

Soit p un entier supérieur ou égal à 2. Montrer que : $(p-1)! \equiv -1 \pmod{p} \Rightarrow p$ est premier (en fait les deux phrases sont équivalentes mais en Sup, on sait trop peu de choses en arithmétique pour pouvoir fournir une démonstration raisonnablement courte de la réciproque).

[Correction ▼](#)

[005312]

Correction de l'exercice 1 ▲

Soit n un entier naturel.

$$n(n+1)(n+2)(n+3) + 1 = n^4 + 6n^3 + 11n^2 + 6n + 1 = (n^2 + 3n + 1)^2,$$

avec $n^2 + 3n + 1$ entier naturel.

Correction de l'exercice 2 ▲

1. Soit n un entier relatif.

Si n est pair, n et $5n^3$ sont pairs de même que $5n^3 + n$ et 2 divise $5n^3 + n$.

Si n est impair, n et $5n^3$ sont impairs et de nouveau $5n^3 + n$ est pair. Finalement : $\forall n \in \mathbb{Z}, 2 \mid (5n^3 + n)$.

Si n est multiple de 3, n et $5n^3$ sont multiples de 3 de même que $5n^3 + n$.

Si n est de la forme $3p + 1$, alors

$$5n^2 + 1 = 5(3p + 1)^2 + 1 = 45p^2 + 30p + 6 = 3(9p^2 + 10p + 2)$$

et $5n^2 + 1$ est divisible par 3. Il en est de même de $5n^3 + n = n(5n^2 + 1)$.

Si n est de la forme $3p + 2$, $5n^2 + 1 = 5(3p + 2)^2 + 1 = 45p^2 + 60p + 21 = 3(9p^2 + 20p + 7)$ et $5n^2 + 1$ est divisible par 3. Il en est de même de $5n^3 + n = n(5n^2 + 1)$.

Finalement, $\forall n \in \mathbb{Z}, 3 \mid (5n^3 + n)$.

Enfin, $5n^3 + n$ est divisible par 2 et 3 et donc par $2 \times 3 = 6$. On a montré que : $\forall n \in \mathbb{Z}, 6 \mid (5n^3 + n)$. (Tout ceci s'exprime beaucoup mieux à l'aide de congruences. Par exemple : si $n \equiv 1 \pmod{3}$, $5n^2 + 1 \equiv 5.1^2 + 1 = 6 \equiv 0 \pmod{3}$)

2. 4^{2^n} signifie $(\dots((4^2)^2)\dots)^2$. Etudions la suite de ces élévations au carré successives modulo 7. $4^{2^0} = 4$ est dans $4 + 7\mathbb{Z}$. $4^{2^1} = 16$ est dans $2 + 7\mathbb{Z}$. $4^{2^2} = 16^2 = (7k + 2)^2 = 4 + 7k'$ est dans $4 + 7\mathbb{Z}$... Montrons par récurrence sur p entier naturel que : $\forall p \in \mathbb{N}, 4^{2^{2p}}$ est dans $4 + 7\mathbb{Z}$ et $4^{2^{2p+1}}$ est dans $2 + 7\mathbb{Z}$.

C'est vrai pour $p = 0$.

Soit $p \geq 0$. Si il existe deux entiers relatifs k_{2p} et k_{2p+1} tels que $4^{2^{2p}} = 4 + 7k_{2p}$ et $4^{2^{2p+1}} = 2 + 7k_{2p+1}$, alors :

$$4^{2^{2p+2}} = (4^{2^{2p+1}})^2 = (2 + 7k_{2p+1})^2 = 4 + 7(4k_{2p+1} + 7k_{2p+1}^2) \in 4 + 7\mathbb{Z},$$

puis

$$4^{2^{2p+3}} = (4^{2^{2p+2}})^2 = (4 + 7k_{2p+2})^2 = 16 + 28k_{2p+2} + 49k_{2p+2}^2 = 2 + 7(2 + 4k_{2p+2} + 7k_{2p+2}^2) \in 2 + 7\mathbb{Z}.$$

On a montré par récurrence que si n est pair, 4^{2^n} est dans $4 + 7\mathbb{Z}$ et si n est impair, 4^{2^n} est dans $2 + 7\mathbb{Z}$.

Ensuite $2^{2^0} = 2$ est dans $2 + 7\mathbb{Z}$ puis, pour $n \geq 1$, $2^{2^n} = 2^{2 \cdot 2^{n-1}} = 4^{2^{n-1}}$ est dans $4 + 7\mathbb{Z}$ si $n - 1$ est pair ou encore si n est impair et est dans $2 + 7\mathbb{Z}$ si n est pair. Ainsi, que n soit pair ou impair, $4^{2^n} + 2^{2^n} + 1$ est dans $(4 + 2) + 1 + 7\mathbb{Z} = 7 + 7\mathbb{Z} = 7\mathbb{Z}$ et on a montré que :

$$\forall n \in \mathbb{N}, 7 \mid 4^{2^n} + 2^{2^n} + 1.$$

Correction de l'exercice 3 ▲

Soient m, n et p trois entiers naturels et r_1, r_2 et r_3 les restes des divisions euclidiennes de m, n et p par 8. Alors,

$$m^2 + n^2 + p^2 = (8q_1 + r_1)^2 + (8q_2 + r_2)^2 + (8q_3 + r_3)^2 \in r_1^2 + r_2^2 + r_3^2 + 8\mathbb{Z}.$$

Donc $m^2 + n^2 + p^2$ est dans $7 + 8\mathbb{Z}$ si et seulement si $r_1^2 + r_2^2 + r_3^2$ est dans $7 + 8\mathbb{Z}$.

Comme r_1, r_2 et r_3 sont des entiers entre 0 et 7, il suffit de vérifier que les sommes de trois carrés d'entiers compris au sens large entre 0 et 7 ne sont pas dans $7 + 8\mathbb{Z}$.

Or, $0^2 = 0 \in 8\mathbb{Z}$, $1^2 = 1 \in 1 + 8\mathbb{Z}$, $2^2 = 4 \in 4 + 8\mathbb{Z}$, $3^2 = 9 \in 1 + 8\mathbb{Z}$, $4^2 = 16 \in 8\mathbb{Z}$, $5^2 = 25 \in 1 + 8\mathbb{Z}$, $6^2 = 36 \in 4 + 8\mathbb{Z}$ et $7^2 = 49 \in 1 + 8\mathbb{Z}$. Donc, les carrés des entiers de 0 à 7 sont dans $8\mathbb{Z}$ ou $1 + 8\mathbb{Z}$ ou $4 + 8\mathbb{Z}$. Enfin,

$$\begin{array}{llll} 0+0+0=0 \in 8\mathbb{Z}, & 0+0+1=1 \in 1+8\mathbb{Z}, & 0+0+4=4 \in 4+8\mathbb{Z}, & 0+1+1=2 \in 2+8\mathbb{Z}, \\ 0+1+4=5 \in 5+8\mathbb{Z} & 0+4+4=8 \in 8\mathbb{Z}, & 1+1+1=3 \in 3+8\mathbb{Z}, & 1+1+4=6 \in 6+8\mathbb{Z}, \\ 1+4+4=9 \in 1+8\mathbb{Z}, & 4+4+4=12 \in 4+8\mathbb{Z}. & & \end{array}$$

Aucune de ces sommes n'est dans $7 + 8\mathbb{Z}$ et on a montré qu'un entier de la forme $8n + 7$ n'est pas la somme de trois carrés.

Correction de l'exercice 4 ▲

Soit $n \in \mathbb{N}^*$. En développant $(1 + \sqrt{2})^n$ par la formule du binôme de NEWTON et en séparant les termes où $\sqrt{2}$ apparaît à un exposant pair des termes où $\sqrt{2}$ apparaît à un exposant impair, on écrit $(1 + \sqrt{2})^n$ sous la forme $a_n + b_n\sqrt{2}$ où a_n et b_n sont des entiers naturels non nuls.

Mais alors $(1 - \sqrt{2})^n = a_n - b_n\sqrt{2}$ et donc

$$(-1)^n = (1 + \sqrt{2})^n (1 - \sqrt{2})^n = (a_n + b_n\sqrt{2})(a_n - b_n\sqrt{2}) = a_n^2 - 2b_n^2$$

ou finalement,

$$((-1)^n a_n) a_n + (2(-1)^{n+1} b_n) b_n = 1$$

où $(-1)^n a_n = u$ et $2(-1)^{n+1} b_n = v$ sont des entiers relatifs. Le théorème de BEZOUT permet d'affirmer que a_n et b_n sont premiers entre eux.

Correction de l'exercice 5 ▲

Posons $(1 + \sqrt{3})^n = a_n + b_n\sqrt{3}$ où a_n et b_n sont des entiers naturels. On a alors $(1 - \sqrt{3})^n = a_n - b_n\sqrt{3}$ et donc

$$(1 + \sqrt{3})^{2n+1} + (1 - \sqrt{3})^{2n+1} = 2a_{2n+1} \in \mathbb{N}.$$

Mais de plus, $-1 < 1 - \sqrt{3} < 0$ et donc, puisque $2n + 1$ est impair, $-1 < (1 - \sqrt{3})^{2n+1} < 0$. Par suite,

$$2a_{2n+1} < (1 + \sqrt{3})^{2n+1} < 2a_{2n+1} + 1,$$

ce qui montre que $E((1 + \sqrt{3})^{2n+1}) = 2a_{2n+1} = (1 + \sqrt{3})^{2n+1} + (1 - \sqrt{3})^{2n+1}$ et montre déjà que $E((1 + \sqrt{3})^{2n+1})$ est un entier pair. Mais on en veut plus :

$$\begin{aligned} (1 + \sqrt{3})^{2n+1} + (1 - \sqrt{3})^{2n+1} &= (1 + \sqrt{3})((1 + \sqrt{3})^2)^n + (1 - \sqrt{3})((1 - \sqrt{3})^2)^n \\ &= (1 + \sqrt{3})(4 + 2\sqrt{3})^n + (1 - \sqrt{3})(4 - 2\sqrt{3})^n \\ &= 2^n((1 + \sqrt{3})(2 + \sqrt{3})^n + (1 - \sqrt{3})(2 - \sqrt{3})^n) \end{aligned}$$

Montrons enfin que $(1 + \sqrt{3})(2 + \sqrt{3})^n + (1 - \sqrt{3})(2 - \sqrt{3})^n$ est un entier, pair. Mais, $(1 + \sqrt{3})(2 + \sqrt{3})^n$ est de la forme $A + B\sqrt{3}$ où A et B sont des entiers naturels et donc, puisque $(1 - \sqrt{3})(2 - \sqrt{3})^n = A - B\sqrt{3}$, on a finalement $(1 + \sqrt{3})(2 + \sqrt{3})^n + (1 - \sqrt{3})(2 - \sqrt{3})^n = 2A$ où A est un entier.

Donc, $(1 + \sqrt{3})(2 + \sqrt{3})^n + (1 - \sqrt{3})(2 - \sqrt{3})^n$ est un entier pair, ou encore $(1 + \sqrt{3})^{2n+1} + (1 - \sqrt{3})^{2n+1} = E((1 + \sqrt{3})^{2n+1})$ est un entier divisible par 2^{n+1} .

Correction de l'exercice 6 ▲

Soit n un entier naturel non nul. On note $\sigma(n)$ la somme de ses chiffres en base 10 (voir l'exercice 19). Si $n = a_0 + 10a_1 + \dots + 10^k a_k$ où $k \in \mathbb{N}$, $0 \leq a_i \leq 9$ pour $0 \leq i \leq k$ et $a_k \neq 0$, alors

$$\sigma(n) = a_0 + \dots + a_k \leq 9(k+1) \leq 9(E(\log n) + 1) \leq 9(\log n + 1).$$

Donc,

$$A = \sigma(4444^{4444}) \leq 9(\log(4444^{4444}) + 1) \leq 9(4444 \log(10^5) + 1) = 9(4444.5 + 1) = 9.22221 = 199989.$$

Puis, $B = \sigma(A) \leq 1 + 5.9 = 46$, puis $\sigma(B) \leq \sigma(39) = 12$. Donc, $1 \leq \sigma(B) \leq 12$.

D'autre part, on sait que modulo 9 : $\sigma(B) \equiv B \equiv A = 4444^{4444}$. Enfin, $4444^{4444} = (9.443 + 7)^{4444} \equiv 7^{4444} (9)$.

De plus, $7 \equiv -2 (9)$ puis $7^2 \equiv 4 (9)$ puis $7^3 \equiv 28 \equiv 1 (9)$ et donc $7^{4444} = (7^3)^{1481} \cdot 7 \equiv (1^3)^{1481} \cdot 7 \equiv 7 (9)$.

Finalement, $1 \leq \sigma(B) \leq 12$ et $C \equiv 7 (9)$ ce qui impose $C = 7$.

Correction de l'exercice 7 ▲

On a trois possibilités : $p \in 3\mathbb{Z}$, $p \in 3\mathbb{Z} + 1$ ou $p \in 3\mathbb{Z} - 1$.

Dans les deux derniers cas, $p^2 \in 1 + 3\mathbb{Z}$ et $8p^2 + 1 \in 9 + 3\mathbb{Z} = 3\mathbb{Z}$. Mais alors, $8p^2 + 1$ est premier et multiple de 3 ce qui impose $8p^2 + 1 = 3$. Cette dernière égalité est impossible.

Il ne reste donc que le cas où p est premier et multiple de 3, c'est-à-dire $p = 3$ (en résumé, p et $8p^2 + 1$ premiers impliquent $p = 3$). Dans ce cas, $8p^2 + 1 = 73$ et $8p^2 - 1 = 71$ sont effectivement premiers.

Correction de l'exercice 8 ▲

1. Pour $1 \leq k \leq n$, $kC_n^k = nC_{n-1}^{k-1}$. Donc, si k et n sont premiers entre eux, puisque n divise kC_n^k , le théorème de GAUSS permet d'affirmer que n divise C_n^k .
2. De même, $(n+1)C_{2n}^{n-1} = nC_{2n}^n$ montre que $(n+1)$ divise nC_{2n}^n et, puisque n et $(n+1)$ sont premiers entre eux (d'après BEZOUT puisque $(n+1) - n = 1$), $(n+1)$ divise C_{2n}^n d'après le théorème de GAUSS.

Correction de l'exercice 9 ▲

1. Posons $d = x \wedge y$ et $m = x \vee y$. d divise $m = 105 = 3.5.7$ mais, puisque d divise x et y , d divise aussi $x + y = 56 = 2^3.7$. Donc, d divise $105 \wedge 56 = 7$ et nécessairement $d = 1$ ou $d = 7$.
1er cas. $d = 1$ fournit, puisque $m = 105$, $xy = md = 105$. x et y sont donc les solutions de l'équation $X^2 - 56X + 105 = 0$ qui n'admet pas de solutions entières.
2ème cas. $d = 7$ fournit $xy = 7.105 = 735$. x et y sont donc les solutions de l'équation $X^2 - 56X + 735 = 0$ qui admet les solutions 21 et 35.
Réciproquement, $21 + 35 = 56$ et $21 \vee 35 = 3.5.7 = 105$. $\mathcal{S} = \{(21, 35), (35, 21)\}$.
2. On pose $x = dx'$ et $y = dy'$ avec x' et y' premiers entre eux et $d = x \wedge y$. Le système s'écrit $\begin{cases} x' - y' = 1 \\ dx'y' = 72 \end{cases}$
ou encore $\begin{cases} x' = y' + 1 \\ d(y' + 1)y' = 72 \end{cases}$. En particulier, y' et $y' + 1$ sont deux diviseurs consécutifs de 72. $72 = 2^3.3^2$ admet 4.3 = 12 diviseurs à savoir 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36 et 72. Donc y' est élément de $\{1, 2, 3, 8\}$.
1er cas. $y' = 1$ fournit $d = \frac{72}{1.2} = 36$ puis $y = 36.1 = 36$ et $x = y + d = 72$. Réciproquement, $72 - 36 = 36 = 36 \wedge 72$ et $36 \vee 72 = 72$.
2ème cas. $y' = 2$ fournit $d = 12$, $y = 24$, $x = 36$ qui réciproquement conviennent.
3ème cas. $y' = 3$ fournit $d = 6$, $y = 18$, $x = 24$ qui réciproquement conviennent.
4ème cas. $y' = 8$ fournit $d = 1$, $y = 8$, $x = 9$ qui réciproquement conviennent.

$$\mathcal{S} = \{(9, 8), (24, 18), (36, 24), (72, 36)\}.$$

3. d divise m et donc d divise $243 = 3^5$ et $d \in \{1, 3, 9, 27, 81, 243\}$. On pose alors $x = dx'$, $y = dy'$ avec x' et y' premiers entre eux.
1er cas. Si $d = 1$ on a $x'y' - 1 = 243$ ou encore $x'y' = 244$ ce qui fournit les possibilités (en n'oubliant pas que x' et y' sont premiers entre eux) :
 $x' = 1$, $y' = 244$ puis $x = 1$ et $y = 244$,

$x' = 4, y' = 61$ puis $x = 4$ et $y = 61$,
 $x' = 61, y' = 4$ puis $x = 61$ et $y = 4$,
 $x' = 244, y' = 1$ puis $x = 244$ et $y = 1$ qui réciproquement conviennent.
 2ème cas. Si $d = 3$, on a $x'y' = 81 + 1 = 82$ ce qui fournit les possibilités :
 $x' = 1, y' = 82$ puis $x = 3$ et $y = 246$,
 $x' = 2, y' = 41$ puis $x = 6$ et $y = 123$,
 $x' = 41, y' = 2$ puis $x = 123$ et $y = 6$,
 $x' = 82, y' = 1$ puis $x = 246$ et $y = 3$ qui réciproquement conviennent.
 3ème cas. Si $d = 9$ on a $x'y' = 27 + 1 = 28$ ce qui fournit les possibilités :
 $x' = 1, y' = 28$ puis $x = 9$ et $y = 252$,
 $x' = 4, y' = 7$ puis $x = 36$ et $y = 63$,
 $x' = 7, y' = 4$ puis $x = 63$ et $y = 36$,
 $x' = 28, y' = 1$ puis $x = 252$ et $y = 9$ qui réciproquement conviennent.
 4ème cas. Si $d = 27$ on a $x'y' = 9 + 1 = 10$ ce qui fournit les possibilités :
 $x' = 1, y' = 10$ puis $x = 27$ et $y = 270$,
 $x' = 2, y' = 5$ puis $x = 54$ et $y = 135$,
 $x' = 5, y' = 2$ puis $x = 135$ et $y = 54$,
 $x' = 10, y' = 1$ puis $x = 270$ et $y = 27$ qui réciproquement conviennent.
 5ème cas. Si $d = 81$, on a $x'y' = 3 + 1 = 4$ ce qui fournit les possibilités :
 $x' = 1, y' = 4$ puis $x = 81$ et $y = 324$,
 $x' = 4, y' = 1$ puis $x = 324$ et $y = 81$ qui réciproquement conviennent.
 6ème cas. Si $d = 243$, on a $x'y' = 1 + 1 = 2$ ce qui fournit les possibilités :
 $x' = 1, y' = 2$ puis $x = 243$ et $y = 486$,
 $x' = 2, y' = 1$ puis $x = 486$ et $y = 243$ qui réciproquement conviennent.

Correction de l'exercice 10 ▲

Soit n un entier supérieur ou égal à 2.

$$(n-2)^2 + (n-1)^2 + n^2 + (n+1)^2 + (n+2)^2 = 5n^2 + 10 = 5(n^2 + 2).$$

$5(n^2 + 2)$ devant être un carré parfait, $n^2 + 2$ doit encore être divisible par 5 mais si n est dans $5\mathbb{Z}$, $n^2 + 2$ est dans $2 + 5\mathbb{Z}$, si n est dans $\pm 1 + 5\mathbb{Z}$, $n^2 + 2$ est dans $3 + 5\mathbb{Z}$ et si n est dans $\pm 2 + 5\mathbb{Z}$, $n^2 + 2$ est dans $1 + 5\mathbb{Z}$ et $n^2 + 2$ n'est jamais divisible par 5. Une somme de cinq carrés d'entiers consécutifs n'est donc pas un carré parfait.

Correction de l'exercice 11 ▲

Soient n et m deux entiers naturels tels que $n < m$. Posons $m = n + k$ avec $k > 0$. On note que

$$F_m = 2^{2^{n+k}} + 1 = (2^{2^n})^{2^k} + 1 = (F_n - 1)^{2^k} + 1.$$

En développant l'expression précédente par la formule du binôme de NEWTON et en tenant compte du fait que 2^k est pair puisque k est strictement positif, on obtient une expression de la forme $q.F_n + 1 + 1 = q.F_n + 2$.

Le P.G.C.D. de F_n et F_m doit encore diviser $F_m - q.F_n = 2$ et vaut donc 1 ou 2. Enfin, puisque 2^n et 2^m sont strictement positifs, F_n et F_m sont impairs et leur P.G.C.D. vaut donc 1 (ce résultat redémontre l'existence d'une infinité de nombres premiers).

Correction de l'exercice 12 ▲

1. Soit, pour n entier naturel non nul donné, $v_n = u_{n+1}u_{n-1} - u_n^2$. Alors,

$$v_{n+1} = u_{n+2}u_n - u_{n+1}^2 = (u_n + u_{n+1})u_n - u_{n+1}(u_{n-1} + u_n) = u_n^2 - u_{n+1}u_{n-1} = -v_n.$$

La suite v est donc une suite géométrique de raison -1 et on a :

$$\forall n \in \mathbb{N}^*, v_n = (-1)^{n-1} v_1 = (-1)^n.$$

Cette égalité s'écrit encore $((-1)^n u_{n-1})u_{n+1} + ((-1)^{n+1} u_n)u_n = 1$ et le théorème de BEZOUT permet d'affirmer que pour tout entier naturel n , les entiers u_n et u_{n+1} sont premiers entre eux (il est clair par récurrence que la suite u est à valeurs entières).

2. Pour $m = 1$ et n entier naturel quelconque :

$$u_{n+m} = u_{n+1} = u_{n+1}u_1 + u_n u_0 = u_{n+1}u_m + u_{m-1}u_n.$$

Pour $m = 2$ et n entier naturel quelconque :

$$u_{n+m} = u_{n+2} = u_{n+1} + u_n = u_{n+1}u_2 + u_n u_1 = u_{n+1}u_m + u_{m-1}u_n.$$

Soit $m \geq 1$. Supposons que pour tout entier naturel n , on a $u_{n+m} = u_{n+1}u_m + u_{m-1}u_n$ et $u_{n+m+1} = u_{n+1}u_{m+1} + u_m u_n$. Alors, pour tout entier naturel n ,

$$\begin{aligned} u_{n+m+2} &= u_{n+m+1} + u_{n+m} = u_{n+1}u_{m+1} + u_m u_n + u_{n+1}u_m + u_{m-1}u_n \text{ (par hypothèse de récurrence)} \\ &= u_{n+1}(u_{m+1} + u_m) + u_n(u_m + u_{m-1}) = u_{n+1}u_{m+2} + u_n u_{m+1}. \end{aligned}$$

ce qui démontre l'égalité proposée par récurrence.

Soient n et m deux entiers naturels tels que $n \geq m$. La division euclidienne de n par m s'écrit $n = mq + r$ avec q et r entiers tels que $0 \leq r \leq m - 1$.

Or, $u_{m+r} = u_m u_{r+1} + u_{m-1} u_r$. Par suite, un diviseur commun à u_m et u_r divise encore u_m et u_{m+r} et réciproquement un diviseur commun à u_m et u_{m+r} divise $u_{m-1} u_r$. Mais, u_m et u_{m-1} sont premiers entre eux et, d'après le théorème de GAUSS, un diviseur commun à u_m et u_{m+r} divise u_r . Les diviseurs communs à u_m et u_r sont encore les diviseurs communs à u_m et u_{m+r} et donc :

$$u_m \wedge u_r = u_m \wedge u_{m+r}.$$

Puis, par récurrence

$$u_m \wedge u_r = u_m \wedge u_{m+r} = u_m \wedge u_{2m+r} = \dots = u_m \wedge u_{qm+r} = u_m \wedge u_n.$$

Ainsi, les algorithmes d'EUCLIDE appliqués d'une part à u_m et u_n et d'autre part à m et n s'effectuent en parallèle et en particulier, $u_m \wedge u_n = u_{m \wedge n}$.

Correction de l'exercice 13 ▲

1. Posons $d = x \wedge y \wedge z$ puis $x = dx'$, $y = dy'$ et $z = dz'$ où $x' \wedge y' \wedge z' = 1$.

$$x^2 + y^2 = z^2 \Leftrightarrow d^2(x'^2 + d^2 y'^2) = d^2 z'^2 \Leftrightarrow x'^2 + y'^2 = z'^2,$$

avec $x' \wedge y' \wedge z' = 1$, ce qui montre que l'on peut se ramener au cas où x , y et z sont premiers entre eux.

Supposons donc x , y et z premiers entre eux (dans leur ensemble). Soit p un nombre premier. Si p divise x et y alors p divise $x^2 + y^2 = z^2$ et donc p est également un facteur premier de z contredisant le fait que x , y et z sont premiers entre eux. Donc, x et y sont premiers entre eux.

Si p divise x et z alors p divise $z^2 - x^2 = y^2$ et donc p est également un facteur premier de y , contredisant le fait que x , y et z sont premiers entre eux. Donc, x et z sont premiers entre eux. De même, y et z sont premiers entre eux. Finalement, x , y et z sont premiers entre eux deux à deux.

2. Puisque x , y et z sont deux à deux premiers entre eux, parmi les nombres x , y et z , il y a au plus un nombre pair. Mais si ces trois nombres sont impairs, $x^2 + y^2 = z^2$ est pair en tant que somme de deux nombres impairs contredisant le fait que z est impair. Ainsi, parmi les nombres x , y et z , il y a exactement un nombre pair et deux nombres impairs.

Si x et y sont impairs, alors d'une part, z est pair et z^2 est dans $4\mathbb{Z}$ et d'autre part x^2 et y^2 sont dans $1 + 4\mathbb{Z}$. Mais alors, $x^2 + y^2$ est dans $2 + 4\mathbb{Z}$ excluant ainsi l'égalité $x^2 + y^2 = z^2$. Donc, z est impair et l'un des deux nombres x ou y est pair. Supposons, quitte à permuter les lettres x et y , que x est impair et y est pair. Posons alors $y = 2y'$ puis $X = \frac{z+x}{2}$ et $Z = \frac{z-x}{2}$ (puisque x et z sont impairs, X et Z sont des entiers).

3. On a

$$x^2 + y^2 = z^2 \Leftrightarrow 4y'^2 = (z+x)(z-x) \Leftrightarrow y'^2 = XZ.$$

Un diviseur commun à X et Z divise encore $z = Z + X$ et $x = Z - X$ et est donc égal à ± 1 puisque x et z sont premiers entre eux. X et Z sont des entiers premiers entre eux.

Le produit des deux entiers X et Z est un carré parfait et ces entiers sont premiers entre eux. Donc, un facteur premier de X n'apparaît pas dans Z et apparaît donc dans X à un exposant pair ce qui montre que X est un carré parfait. De même, Z est un carré parfait.

4. Donc, il existe deux entiers relatifs u et v tels que $X = u^2$ et $Z = v^2$. Mais alors, $z = Z + X = u^2 + v^2$ et $x = Z - X = u^2 - v^2$. Enfin, $y^2 = z^2 - x^2 = (u^2 + v^2)^2 - (u^2 - v^2)^2 = 4u^2v^2$ et donc, $y = 2uv$ quitte à remplacer u par $-u$.

En résumé, si $x^2 + y^2 = z^2$ alors il existe $(d, u, v) \in \mathbb{N}^* \times \mathbb{Z} \times \mathbb{Z}$ tel que $x = d(u^2 - v^2)$, $y = 2duv$ et $z = d(u^2 + v^2)$ ou bien $x = 2duv$, $y = d(u^2 - v^2)$ et $z = d(u^2 + v^2)$.

Réciproquement,

$$(d(u^2 - v^2))^2 + (2duv)^2 = d^2(u^4 + 2u^2v^2 + v^4) = (d(u^2 + v^2))^2,$$

et on a trouvé tous les triplets Pythagoriciens. Par exemple, $d = 1$, $u = 2$ et $v = 1$ fournissent le triplet $(3, 4, 5)$. $d = 2$, $u = 2$ et $v = 1$ fournissent le triplet $(6, 8, 10)$ et $d = 1$, $u = 3$ et $v = 2$ fournissent le triplet $(5, 12, 13)$.

Correction de l'exercice 14 ▲

Soient x et y deux entiers naturels tels que $3x^3 + xy + 4y^3 = 349$. On a $4y^3 \leq 3x^3 + xy + 4y^3 = 349$ et donc

$$y \leq \sqrt[3]{\frac{349}{4}} = 4,4\dots$$

Donc, $y \in \{0, 1, 2, 3, 4\}$. De même, $3x^3 \leq 3x^3 + xy + 4y^3 = 349$ et donc

$$x \leq \sqrt[3]{\frac{349}{3}} = 4,8\dots$$

Donc, $x \in \{0, 1, 2, 3, 4\}$ ce qui ne laisse plus que $5 \cdot 5 = 25$ couples candidats. Ensuite,

$y = 0$ donne $3x^3 = 349$ qui ne fournit pas de solutions.

$y = 1$ donne $3x^3 + x - 345 = 0$, équation dont aucun des entiers de 0 à 4 n'est solution.

$y = 2$ donne $3x^3 + 2x - 317 = 0$, équation dont aucun des entiers de 0 à 4 n'est solution.

$y = 3$ donne $3x^3 + 3x - 241 = 0$, équation dont aucun des entiers de 0 à 4 n'est solution.

$y = 4$ donne $3x^3 + 4x - 93 = 0$ dont seul $x = 3$ est solution.

$$\mathcal{S} = \{(3, 4)\}.$$

Correction de l'exercice 15 ▲

Si $x \geq 5$ et $5 \leq k \leq x$, alors $k!$ est divisible par $2 \cdot 5 = 10$. D'autre part, $1! + 2! + 3! + 4! = 33$ et le chiffre des unités de $\sum_{k=1}^x k!$ est 3. $\sum_{k=1}^x k!$ n'est donc pas un carré parfait car le chiffre des unités (en base 10) d'un carré

parfait est à choisir parmi 0, 1, 4, 5, 6, 9. Donc, $x \leq 4$. Ensuite, $1! = 1 = 1^2$ puis $1! + 2! = 1 + 2 = 3$ n'est pas un carré parfait, puis $1! + 2! + 3! = 9 = 3^2$ puis $1! + 2! + 3! + 4! = 33$ n'est pas un carré parfait.

$$\mathcal{S} = \{(1, 1), (3, 3)\}.$$

Correction de l'exercice 16 ▲

$$\begin{aligned} n &= 9 + 8(10 + 10^2 + \dots + 10^{p-1}) + 4(10^p + \dots + 10^{2p-1}) = 9 + 80 \frac{10^{p-1} - 1}{10 - 1} + 4 \cdot 10^p \frac{10^p - 1}{10 - 1} \\ &= \frac{1}{9}(81 + 80(10^{p-1} - 1) + 4 \cdot 10^p(10^p - 1)) = \frac{1}{9}(4 \cdot 10^{2p} + 4 \cdot 10^p + 1) = \left(\frac{2 \cdot 10^p + 1}{3}\right)^2, \end{aligned}$$

(ce qui montre déjà que n est le carré d'un rationnel). Maintenant,

$$2 \cdot 10^p + 1 = 2(9 + 1)^p + 1 = 2 \cdot \sum_{k=0}^p C_p^k 9^k + 1 = 3 + 2 \sum_{k=1}^p C_p^k 3^{2k} = 3(1 + 2 \sum_{k=1}^p C_p^k 3^{2k-1}),$$

et $2 \cdot 10^p + 1$ est un entier divisible par 3. Finalement, $n = \left(\frac{2 \cdot 10^p + 1}{3}\right)^2$ est bien le carré d'un entier.

Correction de l'exercice 17 ▲

Pour $k \in \mathbb{N}$, posons $a_k = 11\dots 1$ ($k + 1$ chiffres 1 en base 10).

Soit n un entier naturel quelconque.

La division euclidienne de a_k par n s'écrit : $a_k = n \cdot q_k + r_k$ où q_k et r_k sont des entiers naturels tels que $0 \leq r_k \leq n - 1$.

Les $n + 1$ entiers r_0, \dots, r_n sont à choisir parmi les n entiers $0, 1, \dots, n - 1$. Les $n + 1$ restes considérés ne peuvent donc être deux à deux distincts. Par suite,

$$\exists (k, l) \in \mathbb{N}^2 / 0 \leq k < l \leq n \text{ et } r_k = r_l.$$

Mais alors, $a_l - a_k = (q_l - q_k)n$ est un multiple de n . Comme $a_l - a_k = 11\dots 10\dots 0$ ($l - k$ chiffres 1 et $k + 1$ chiffres 0), on a montré que tout entier naturel admet un multiple de la forme $11\dots 10\dots 0 = 11\dots 1 \cdot 10^K$. Si de plus n est impair, non divisible par 5, alors n est premier à 2 et à 5 et donc à 10^K . D'après le théorème de GAUSS, n divise $11\dots 1$.

Correction de l'exercice 18 ▲

1. $u_n^2 = (2^{n+1} + 1)^2 = 2^{2n+2} + 2^{n+2} + 1 = 10\dots 010\dots 01_2$ ($n - 1$ puis $n + 1$ chiffres 0)

2.

$$\begin{aligned} u_n^3 &= (2^{n+1} + 1)^3 = 2^{3n+3} + 3 \cdot 2^{2n+2} + 3 \cdot 2^{n+1} + 1 = 2^{3n+3} + (2 + 1) \cdot 2^{2n+2} + (2 + 1) \cdot 2^{n+1} + 1 \\ &= 2^{3n+3} + 2^{2n+3} + 2^{2n+2} + 2^{n+2} + 2^{n+1} + 1 = 10\dots 0110\dots 0110\dots 01_2 \end{aligned}$$

($n - 1$ puis $n - 1$ puis n chiffres 0)

3.

$$\begin{aligned} u_n^3 - u_n^2 + u_n &= 2^{3n+3} + 3 \cdot 2^{2n+2} + 3 \cdot 2^{n+1} + 1 - 2^{2n+2} - 2^{n+2} - 1 + 2^{n+1} + 1 = 2^{3n+3} + 2^{2n+3} + 2^{n+2} + 1 \\ &= 10\dots 010\dots 010\dots 01 \end{aligned}$$

($n - 1$ puis n puis $n + 1$ chiffres 0)

Correction de l'exercice 19 ▲

1. Soit $n \in \mathbb{N}^*$. Posons $n = \sum_{k=0}^p a_k 10^k$, où $p \in \mathbb{N}$, et $\forall k \in \{0, \dots, p\}$, $a_k \in \{0, \dots, 9\}$, et $a_p \neq 0$. Le nombre de chiffres de n est alors $p+1$. L'entier p vérifie $10^p \leq n < 10^{p+1}$ ou encore $p \leq \log n < p+1$. Par suite, $p = E(\log n)$. Ainsi, le nombre de chiffres de n en base 10 est $E(\log n) + 1$.
2. Pour $n \in \mathbb{N}^*$, posons $u_n = \frac{\sigma(n+1)}{\sigma(n)}$
 - (a) Soit $n \in \mathbb{N}^*$. Posons $n = a_p 10^p + \dots + 10a_1 + a_0 = \overline{a_p \dots a_1 a_0}_{10}$. Si au moins un des chiffres de n n'est pas 9, on note k le plus petit indice tel que $a_k \neq 9$. Alors, $0 \leq k \leq p-1$ et $n = \overline{a_p \dots a_k 9 \dots 9}_{10}$ et $n+1 = \overline{a_p \dots a_{k+1} (a_k+1) 0 \dots 0}_{10}$. Dans ce cas, si $k=0$,

$$\frac{\sigma(n+1)}{\sigma(n)} = \frac{\sigma(n)+1}{\sigma(n)} = 1 + \frac{1}{\sigma(n)} \leq 1 + 1 = 2.$$

Si $1 \leq k \leq p-1$,

$$\frac{\sigma(n+1)}{\sigma(n)} = \frac{a_p + \dots + a_k + 1}{a_p + \dots + a_k + 9k} \leq \frac{a_p + \dots + a_k + 1}{a_p + \dots + a_k + 1} = 1 \leq 2.$$

Sinon, tous les chiffres de n sont égaux à 9, et dans ce cas,

$$\frac{\sigma(n+1)}{\sigma(n)} = \frac{1}{9(p+1)} \leq 2.$$

Ainsi, pour tout entier naturel non nul n , on a $u_n \leq 2$. La suite u est donc bornée.

Pour $p \in \mathbb{N}^*$, $u_{10^p-1} = \frac{\sigma(10^p)}{\sigma(10^p-1)} = \frac{1}{9^p}$. La suite extraite $(u_{10^p-1})_{p \in \mathbb{N}}$ converge et a pour limite 0.

Pour $p \in \mathbb{N}^*$, $u_{10^p} = \frac{\sigma(10^p+1)}{\sigma(10^p)} = \frac{2}{1} = 2$. La suite extraite $(u_{10^p})_{p \in \mathbb{N}}$ converge et a pour limite $2 \neq 0$. On en déduit que la suite u diverge.

- (b) Avec les notations du a), $1 \leq \sigma(n) \leq 9(p+1) = 9(E(\log n) + 1) \leq 9(\log n + 1)$.
- (c) Soit $n \in \mathbb{N}^*$. $1 \leq \sqrt[n]{\sigma(n)} \leq \sqrt[n]{9(\log n + 1)} = \exp\left(\frac{1}{n}(\ln 9 + \ln(1 + \frac{\ln n}{\ln 10}))\right)$. Les deux membres de cet encadrement tendent vers 1 et donc la suite $(\sqrt[n]{\sigma(n)})_{n \geq 1}$ converge et $\lim_{n \rightarrow +\infty} \sqrt[n]{\sigma(n)} = 1$.

Correction de l'exercice 20 ▲

1. (Formule de LEGENDRE) Soit n un entier naturel supérieur ou égal à 2.

Si p est un nombre premier qui divise $n! = 1.2 \dots n$, alors p est un facteur premier de l'un des entiers $2, \dots, n$ et en particulier, $p \leq n$. Réciproquement, il est clair que si p est un nombre premier tel que $p \leq n$, p divise $n!$. Les facteurs premiers de $n!$ sont donc les nombres premiers inférieurs ou égaux à n .

Soit donc p un nombre premier tel que $p \leq n$. Pour trouver l'exposant de p dans la décomposition primaire de $n!$, on compte 1 pour chaque multiple de p inférieur ou égal à n , on rajoute 1 pour chaque multiple de p^2 inférieur ou égal à n , on rajoute encore 1 pour chaque multiple de p^3 inférieur ou égal à $n \dots$ et on s'arrête quand l'exposant k vérifie $p^k > n$.

$$n \geq p^k \Leftrightarrow \ln n \geq k \ln p \Leftrightarrow k \leq \frac{\ln n}{\ln p},$$

(car $\ln p > 0$). Donc, si $k \geq E(\frac{\ln n}{\ln p}) + 1$, alors $p^k > n$.

Dit autrement, l'exposant de p est la somme du nombre de multiples de p inférieurs ou égaux à n , du nombre de multiples de p^2 inférieurs ou égaux à n , du nombre de multiples de p^3 inférieurs ou égaux à $n \dots$ et du nombre de multiples de $p^{E(\ln n / \ln p)}$.

Soit k un entier tel que $1 \leq k \leq E(\frac{\ln n}{\ln p})$ et K un entier naturel.

$$1 \leq K.p^k \leq n \Leftrightarrow \frac{1}{p^k} \leq K \leq \frac{n}{p^k} \Leftrightarrow 1 \leq K \leq E\left(\frac{n}{p^k}\right).$$

Il y a donc $E(\frac{n}{p^k})$ multiples de p^k compris au sens large entre 1 et n . On a montré que l'exposant de p dans la décomposition de $n!$ en facteurs premiers est

$$E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + E\left(\frac{n}{p^3}\right) + \dots$$

2. L'exposant de 5 dans la décomposition primaire de 1000! est

$$E\left(\frac{1000}{5}\right) + E\left(\frac{1000}{5^2}\right) + E\left(\frac{1000}{5^3}\right) + E\left(\frac{1000}{5^4}\right) = 200 + 40 + 8 + 1 = 249.$$

L'exposant de 2 est évidemment supérieur (il y a déjà au moins 500 nombres pairs entre 1 et 1000). Donc, la plus grande puissance de 10 divisant 1000! est encore la plus grande puissance de 5 divisant 1000!, à savoir 249. L'écriture en base 10 de 1000! se termine par 249 zéros.

Correction de l'exercice 21 ▲

(Petit théorème de FERMAT) Soit p un nombre premier.

1. Soit p un nombre premier et k un entier tel que $1 \leq k \leq p-1$. On a $kC_p^k = pC_{p-1}^{k-1}$. Donc, p divise kC_p^k . Mais, p est premier et donc p est premier à tous les entiers compris entre 1 et $p-1$ au sens large. D'après le théorème de GAUSS, p divise C_p^k .

2. Soit p un nombre premier. Montrons par récurrence que $\forall a \in \mathbb{N}^*, a^p \equiv a \pmod{p}$.

C'est clair pour $a = 1$.

Soit $a \geq 1$. Supposons que $a^p \equiv a \pmod{p}$. On a alors

$$\begin{aligned} (a+1)^p &= \sum_{k=0}^p C_p^k a^k = a^p + 1 + \sum_{k=1}^{p-1} C_p^k a^k \\ &\equiv a^p + 1 \pmod{p} \quad (\text{d'après 1}) \\ &\equiv a + 1 \pmod{p} \quad (\text{par hypothèse de récurrence}) \end{aligned}$$

On a montré par récurrence que $\forall a \in \mathbb{N}^*, a^p \equiv a \pmod{p}$.

Correction de l'exercice 22 ▲

Soit p un entier naturel supérieur ou égal à 2.

Supposons que $(p-1)! \equiv -1 \pmod{p}$. Il existe donc un entier relatif a tel que $(p-1)! = -1 + ap (*)$.

Soit $k \in \{1, \dots, p-1\}$. L'égalité $(*)$ s'écrit encore $k(-\prod_{j \neq k} j) + ap = 1$. Le théorème de BEZOUT permet alors d'affirmer que k et p sont premiers entre eux. Ainsi, p est premier avec tous les entiers naturels éléments de $\{1, \dots, p-1\}$ et donc, p est un nombre premier.