

# Planche n° 16. Arithmétique. Corrigé

**n° 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. Donc

$$\forall n \in \mathbb{N}, n(n+1)(n+2)(n+3)+1 \text{ est un carré parfait.}$$

**n° 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 :  $\forall n \in \mathbb{Z}, 2|(5n^3 + n)$ .

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

Sinon  $n \equiv \pm 1 [3]$ , et

$$5n^2 + 1 \equiv 5 \times (\pm 1)^2 + 1 [3] \text{ ou encore } 5n^2 + 1 \equiv 6 [3] \text{ ou enfin } 5n^2 + 1 \equiv 0 [3].$$

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

Finalement,  $(5n^3 + n)$  est divisible par 3.

Enfin,  $5n^3 + n$  est divisible par 2 et 3 et donc par  $2 \vee 3 = 2 \times 3 = 6$ .

On a montré que :

$$\forall n \in \mathbb{Z}, 6|(5n^3 + n).$$

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 :  $\forall p \in \mathbb{N}, 4^{2^{2^p}}$  est dans  $4 + 7\mathbb{Z}$  et  $4^{2^{2^{p+1}}}$  est dans  $2 + 7\mathbb{Z}$ .

• C'est vrai pour  $p = 0$ .

• Soit  $p \geq 0$ . Supposons que  $4^{2^{2^p}} \equiv 4 [7]$  et  $4^{2^{2^{p+1}}} \equiv 2 [7]$ . Alors :

$$4^{2^{2^{p+2}}} = (4^{2^{2^{p+1}}})^2 \equiv 2^2 [7] \text{ ou encore } 4^{2^{2^{p+2}}} \equiv 4 [7],$$

puis

$$4^{2^{2^{p+3}}} = (4^{2^{2^{p+2}}})^2 \equiv 4^2 [7] \text{ ou encore } 4^{2^{2^{p+3}}} \equiv 2 [7].$$

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 :

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

**n° 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,

$$m^2 + n^2 + p^2 \equiv r_1^2 + r_2^2 + r_3^2 [8].$$

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.

**n° 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. On a aussi  $(1 - \sqrt{2})^n = a_n - b_n\sqrt{2}$  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,

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

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

**n° 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.  $(1 + \sqrt{3})(2 + \sqrt{3})^n$  est de la forme  $A + B\sqrt{3}$  où  $A$  et  $B$  sont des entiers naturels. Un calcul conjugué fournit  $(1 - \sqrt{3})(2 - \sqrt{3})^n = A - B\sqrt{3}$  et donc  $(1 + \sqrt{3})(2 + \sqrt{3})^n + (1 - \sqrt{3})(2 - \sqrt{3})^n = 2A$  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  $2^{n+1}$ .

$$\forall n \in \mathbb{N}, E((1 + \sqrt{3})^{2n+1}) \text{ est un entier divisible par } 2^{n+1}.$$

**n° 6 :** Soit  $n$  un entier naturel non nul. On note  $\sigma(n)$  la somme de ses chiffres en base 10 (voir exercice n° 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,

$$A = \sigma(4444^{4444}) \leq 9(\log(4444^{4444}) + 1) \leq 9(4444 \log(10^5) + 1) = 9(4444 \times 5 + 1) = 9 \times 22221 = 199989.$$

Puis,  $B = \sigma(A) \leq 1 + 5 \times 9 = 46$ , puis  $\sigma(B) \leq \sigma(39) = 12$ . Donc,  $1 \leq \sigma(B) \leq 12$ .

D'autre part, on sait que modulo 9 :  $\sigma(B) \equiv B \equiv A = 4444^{4444}$ . Or,  $4444^{4444} = (9 \times 443 + 7)^{4444} \equiv 7^{4444} \pmod{9}$ . De plus,  $7 \equiv -2 \pmod{9}$  puis  $7^2 \equiv 4 \pmod{9}$  puis  $7^3 \equiv 28 \equiv 1 \pmod{9}$  et donc  $7^{4444} = (7^3)^{1481} \cdot 7 \equiv (1^3)^{1481} \cdot 7 \equiv 7 \pmod{9}$ . Finalement,  $1 \leq \sigma(B) \leq 12$  et  $\sigma(B) \equiv 7 \pmod{9}$  ce qui impose

$$\sigma(B) = 7.$$

**n° 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.

**n° 8 :** 1) Pour  $1 \leq k \leq n$ ,  $kC_n^k = nC_{n-1}^{k-1}$ . Puisque  $n$  divise  $nC_{n-1}^{k-1}$ ,  $n$  divise encore  $kC_n^k$  et puisque  $k$  et  $n$  sont premiers entre eux, le théorème de GAUSS permet d'affirmer que  $n$  divise  $C_n^k$ .

2) De même, l'égalité  $(n+1)C_{2n}^{n-1} = nC_{2n}^n$  montre que  $(n+1)$  divise  $nC_{2n}^n$  et, puisque  $n$  et  $(n+1)$  sont premiers entre eux (d'après BÉZOUT puisque  $(n+1) - n = 1$ ),  $(n+1)$  divise  $C_{2n}^n$  d'après le théorème de GAUSS.

**n° 9 :** 1) Posons  $d = x \wedge y$  et  $m = x \vee y$ .  $d$  divise  $m = 105 = 3 \times 5 \times 7$  mais, puisque  $d$  divise  $x$  et  $y$ ,  $d$  divise aussi  $x + y = 56 = 2^3 \times 7$ . Donc,  $d$  divise  $105 \wedge 56 = 7$  et nécessairement  $d = 1$  ou  $d = 7$ .

**1er cas.**  $d = 1$  fournit  $xy = md = 105$ .  $x$  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  $xy = 7 \times 105 = 735$ .  $x$  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  $21 \vee 35 = 3 \times 5 \times 7 = 105$ .

$$\mathcal{S} = \{(21, 35), (35, 21)\}.$$

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. Maintenant  $72 = 2^3 \times 3^2$  admet  $4 \times 3 = 12$  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  $d = \frac{72}{1 \times 2} = 36$  puis  $y = 36 \times 1 = 36$  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) :

$$x' = 1, y' = 244 \text{ puis } x = 1 \text{ et } y = 244,$$

$$x' = 4, y' = 61 \text{ puis } x = 4 \text{ et } y = 61,$$

$$x' = 61, y' = 4 \text{ puis } x = 61 \text{ et } y = 4,$$

$$x' = 244, y' = 1 \text{ puis } x = 244 \text{ et } y = 1 \text{ qui réciproquement conviennent.}$$

**2ème cas.** Si  $d = 3$ , on a  $x'y' = 81 + 1 = 82$  ce qui fournit les possibilités :

$$x' = 1, y' = 82 \text{ puis } x = 3 \text{ et } y = 246,$$

$$x' = 2, y' = 41 \text{ puis } x = 6 \text{ et } y = 123,$$

$$x' = 41, y' = 2 \text{ puis } x = 123 \text{ et } y = 6,$$

$$x' = 82, y' = 1 \text{ puis } x = 246 \text{ et } y = 3 \text{ qui réciproquement conviennent.}$$

**3ème cas.** Si  $d = 9$  on a  $x'y' = 27 + 1 = 28$  ce qui fournit les possibilités :

$$x' = 1, y' = 28 \text{ puis } x = 9 \text{ et } y = 252,$$

$$x' = 4, y' = 7 \text{ puis } x = 36 \text{ et } y = 63,$$

$$x' = 7, y' = 4 \text{ puis } x = 63 \text{ et } y = 36,$$

$$x' = 28, y' = 1 \text{ puis } x = 252 \text{ et } y = 9 \text{ qui réciproquement conviennent.}$$

**4ème cas.** Si  $d = 27$  on a  $x'y' = 9 + 1 = 10$  ce qui fournit les possibilités :

$$x' = 1, y' = 10 \text{ puis } x = 27 \text{ et } y = 270,$$

$$x' = 2, y' = 5 \text{ puis } x = 54 \text{ et } y = 135,$$

$$x' = 5, y' = 2 \text{ puis } x = 135 \text{ et } y = 54,$$

$$x' = 10, y' = 1 \text{ puis } x = 270 \text{ et } y = 27 \text{ qui réciproquement conviennent.}$$

**5ème cas.** Si  $d = 81$ , on a  $x'y' = 3 + 1 = 4$  ce qui fournit les possibilités :

$$x' = 1, y' = 4 \text{ puis } x = 81 \text{ et } y = 324,$$

$$x' = 4, y' = 1 \text{ puis } x = 324 \text{ et } y = 81 \text{ qui réciproquement conviennent.}$$

**6ème cas.** Si  $d = 243$ , on a  $x'y' = 1 + 1 = 2$  ce qui fournit les possibilités :

$$x' = 1, y' = 2 \text{ puis } x = 243 \text{ et } y = 486,$$

$$x' = 2, y' = 1 \text{ puis } x = 486 \text{ et } y = 243 \text{ qui réciproquement conviennent.}$$

$\mathcal{S} = \{(1, 244), (4, 61), (61, 4), (244, 1), (3, 246), (6, 123), (123, 6), (246, 3), (9, 252), (36, 63), (63, 36), (252, 9), (27, 270), (54, 135), (135, 54), (270, 27), (81, 324), (324, 81), (243, 486), (486, 243)\}$ .

**n° 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  $1 + 5\mathbb{Z}$ . Ainsi,  $n^2 + 2$  n'est jamais divisible par 5 et donc une somme de cinq carrés d'entiers consécutifs n'est donc pas un carré parfait.

**n° 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  $q \times F_n + 1 + 1 = q \times F_n + 2$ .

Le P.G.C.D. de  $F_n$  et  $F_m$  doit encore diviser  $F_m - q \times F_n = 2$  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).

**n° 12 :** 1) Pour  $n$  entier naturel non nul donné, on pose  $v_n = u_{n+1}u_{n-1} - u_n^2$ . Pour  $n \in \mathbb{N}^*$ , on a

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

La suite  $v$  est une suite géométrique de raison  $-1$  et donc

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

Cette égalité s'écrit encore  $((-1)^n u_{n+1}) \times u_{n-1} + ((-1)^{n+1} u_n) \times u_n = 1$  et le théorème de BÉZOUT 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).

$$\forall n \in \mathbb{N}, u_n \wedge u_{n+1} = 1.$$

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,

$$\forall (m, n) \in (\mathbb{N}^*)^2, u_m \wedge u_n = u_{m \wedge n}.$$

**n° 13 :** 1) Posons  $d = x \wedge y \wedge z$  puis  $x = dx'$ ,  $y = dy'$  et  $z = dz'$  où  $x' \wedge y' \wedge z' = 1$ .

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

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  $\pm 1$  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. On en déduit qu'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  $(5, 12, 13)$ .

**n° 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  $5 \times 5 = 25$  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.

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

**n° 15 :** Si  $x \geq 5$  et  $5 \leq k \leq x$ , alors  $k!$  est divisible par  $2 \times 5 = 10$ . 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.

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

**n° 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,

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

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.

**n° 17 :** Pour  $k \in \mathbb{N}$ , posons  $a_k = \underbrace{11\dots1}_{k+1}$  ( $k + 1$  chiffres 1 en base 10).

Soit  $n$  un entier naturel non nul quelconque.

La division euclidienne de  $a_k$  par  $n$  s'écrit :  $a_k = n \times q_k + r_k$  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, ...,  $n - 1$ . 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  $a_l - a_k = 11\dots10\dots0$  ( $l - k$  chiffres 1 et  $k + 1$  chiffres 0), on a montré que tout entier naturel admet un multiple de la forme  $11\dots10\dots0 = 11\dots1 \times 10^k$ . 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  $11\dots1$ .

Par exemple,  $37 \times 1 = 37$ ,  $37 \times 2 = 74$ ,  $37 \times 3 = 111$ .

**n° 18 :** 1) Soit  $n \in \mathbb{N}^*$ .  $u_n^2 = (2^{n+1} + 1)^2 = 2^{2n+2} + 2^{n+2} + 1 = 10\dots010\dots01_2$  ( $n - 1$  puis  $n + 1$  chiffres 0). D'autre part,  $u_0^2 = 3^2 = 9 = 1001_2$ .

2) Soit  $n \in \mathbb{N}^*$ .

$$\begin{aligned}
 u_n^3 &= (2^{n+1} + 1)^3 = 2^{3n+3} + 3 \times 2^{2n+2} + 3 \times 2^{n+1} + 1 = 2^{3n+3} + (2 + 1)2^{2n+2} + (2 + 1)2^{n+1} + 1 \\
 &= 2^{3n+3} + 2^{2n+3} + 2^{2n+2} + 2^{n+2} + 2^{n+1} + 1 = 10\dots0110\dots0110\dots01_2
 \end{aligned}$$

( $n - 1$  puis  $n - 1$  puis  $n$  chiffres 0). D'autre part,  $u_0^3 = 3^3 = 27 = 11011_2$ .

3) Soit  $n \in \mathbb{N}^*$ .

$$\begin{aligned}
 u_n^3 - u_n^2 + u_n &= 2^{3n+3} + 3 \times 2^{2n+2} + 3 \times 2^{n+1} + 1 - 2^{2n+2} - 2^{n+2} - 1 + 2^{n+1} + 1 = 2^{3n+3} + 2^{2n+3} + 2^{n+1} + 1 \\
 &= 10\dots010\dots010\dots01
 \end{aligned}$$

( $n - 1$  puis  $n + 1$  puis  $n$  chiffres 0). D'autre part,  $u_0^3 = 3^3 - 3^2 + 3 = 21 = 10101_2$ .

**n° 19 :** 1) Soit  $n \in \mathbb{N}^*$ . Posons  $n = \sum_{k=0}^p a_k 10^k$ , où  $p \in \mathbb{N}$ , et  $\forall k \in \llbracket 0, p \rrbracket$ ,  $a_k \in \{0, \dots, 9\}$ , 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,  $p = E(\log n)$  et 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,  $0 \leq k \leq p$  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  $k = 0$ ,

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

- et si  $1 \leq k \leq p$ ,

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

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

**n° 20 :** 1) (**Formule de LEGENDRE**) Soit  $n$  un entier naturel supérieur ou égal à 2.

Si  $p$  est un nombre premier qui divise  $n! = 1 \times 2 \times \dots \times n$ , 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  $p^k > n$ . 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  $p^m$  où  $m$  est le plus grand entier  $k$  tel que  $p^k \leq n$ .

Déterminons  $m$ .

$$p^k \leq n \Leftrightarrow k \ln p \leq \ln n \Leftrightarrow k \leq \frac{\ln n}{\ln p} \Leftrightarrow k \leq E\left(\frac{\ln n}{\ln p}\right),$$

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

Soit alors  $k$  un entier tel que  $1 \leq k \leq m$  et  $K$  un entier naturel.

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

Il y a donc  $E\left(\frac{n}{p^k}\right)$  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

$$E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + E\left(\frac{n}{p^3}\right) + \dots + E\left(\frac{n}{p^m}\right) \text{ où } m = E\left(\frac{\ln n}{\ln p}\right).$$

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 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.

**n° 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 et en particulier avec  $k$ . 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

$$\forall a \in \mathbb{N}^*, a^p \equiv a \pmod{p}.$$

**n° 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  $k \in \llbracket 1, p-1 \rrbracket$ . L'égalité (\*) s'écrit encore  $k \left( - \prod_{j \neq k} j \right) + ap = 1$ . 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  $\llbracket 1, p-1 \rrbracket$  et donc,  $p$  est un nombre premier.