Planche n° 24. Arithmétique dans $\mathbb{Z}$. Corrigé

Exercice 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.

Exercice n° 2

1) Soit n un entier relatif.

• Si n est pair, alors $5n^3+n \equiv 5\times 0^3+0$ [2] ou encore $5n^3+n\equiv 0$ [2]. Dans ce cas, $5n^3+n$ est divisible par 2.
Si n est impair,alors $5n^3+n\equiv 5\times 1^3+1$ [2] ou encore $5n^3+n\equiv 6$ [2] ou enfin $5n^3+n\equiv 0$ [2]. Dans ce cas aussi, $5n^3+n$ est divisible par 2. Finalement : $\forall n\in\mathbb{Z},\ 2\mid(5n^3+n)$.

• Si n est multiple de 3, alors $5n^3+n\equiv 5\times 0^3+0$ [3] ou encore $5n^3+n\equiv 0$ [3]. Dans ce cas, $5n^3+n$ est divisible par 3.
Si n est de la forme $3k+1$ où $k\in\mathbb{Z}$, alors

$$5n^3+n\equiv 5\times 1^3+1\ [3] \text{ puis } 5n^3+n\equiv 6\ [3] \text{ et donc } 5n^3+n\equiv 0\ [3].$$

Par suite, $5n^3+n$ est divisible par 3.
Si n est de la forme $3k+2$ où $k\in\mathbb{Z}$, alors ,

$$5n^3+n\equiv 5\times 2^3+2\ [3] \text{ puis } 5n^3+n\equiv 42\ [3] \text{ et donc } 5n^3+n\equiv 0\ [3].$$

Dans ce cas aussi, $5n^3+n$ est divisible par 3.

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

Enfin, pour tout $n\in\mathbb{Z}$, $5n^3+n$ est divisible par les nombres premiers 2 et 3 et donc par $2\times 3=6$. On a montré que

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

2) 4^{2^n} signifie $(...((4^2)^2)^2...)^2$. Etudions la suite de ces élévations au carré successives modulo 7.
$4^{2^0}=4$ et donc $4^{2^0}\equiv 4$ [7]. Ensuite, $4^{2^1}\equiv 4^2$ [7] ou encore $4^{2^1}\equiv 2$ [7]. Ensuite, $4^{2^2}\equiv 2^2$ [7] ou encore $4^{2^2}\equiv 4$ [7] ...

Montrons par récurrence que : $\forall k\in\mathbb{N}$, $4^{2^{2k}}\equiv 4$ [7] et $4^{2^{2k+1}}\equiv 2$ [7].

• C'est vrai pour $k=0$.
• Soit $k\geqslant 0$. Supposons que $4^{2^{2k}}\equiv 4$ [7] et $4^{2^{2k+1}}\equiv 2$ [7].
Alors, $4^{2^{2(k+1)}}=\left(4^{2^{2k+1}}\right)^2\equiv 2^2$ [7] ou encore $4^{2^{2(k+1)}}\equiv 4$ [7] puis $4^{2^{2(k+1)+1}}=\left(4^{2^{2(k+1)}}\right)^2\equiv 4^2$ [7] ou encore $4^{2^{2(k+1)+1}}\equiv 2$ [7]

On a montré par récurrence que $\forall k\in\mathbb{N}$, $4^{2^{2k}}\equiv 4$ [7] et $4^{2^{2k+1}}\equiv 2$ [7].

Ensuite $2^{2^0}=2$ est dans $2+7\mathbb{Z}$ puis, pour $n\geqslant 1$, $2^{2^n}=2^{2\times 2^{n-1}}=4^{2^{n-1}}$ 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 :

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

Exercice 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.

Exercice n° 4

Soit $n\in\mathbb{N}^*$. En développant $\left(1+\sqrt{2}\right)^n$ 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. Un calcul conjugué fournit $(1-\sqrt{2})^n=a_n-b_n\sqrt{2}$ et donc

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

ou finalement,

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

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

Exercice n° 5

Posons $\left(1+\sqrt{3}\right)^n=a_n+b_n\sqrt{3}$ où a_n et b_n sont des entiers naturels puis $\left(1-\sqrt{3}\right)^n=a_n-b_n\sqrt{3}$ et donc

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

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

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

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

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

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

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

Exercice n° 6

Soit n un entier naturel non nul. On note $\sigma(n)$ la somme de ses chiffres en base 10. Si $n=c_0+10c_1+\ldots+10^kc_k$ où $k\in\mathbb{N}$, $0\leqslant c_i\leqslant 9$ pour $0\leqslant i\leqslant k$ et $c_k\neq 0$, alors

$$\sigma(n)=c_0+\ldots+c_k\leqslant 9(k+1)=9(\lfloor\log n\rfloor+1)\leqslant 9(\log n+1).$$

Donc,

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

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

D'autre part, on sait que modulo 9 : $\sigma(B) \equiv B \equiv A \equiv 4444^{4444}$. Enfin, $4444^{4444} = (9 \times 493 + 7)^{4444} \equiv 7^{4444}$ [9]. De plus, $7 \equiv -2$ [9] puis $7^2 \equiv 4$ [9] puis $7^3 \equiv -8 \equiv 1$ [9] et donc $7^{4444} = (7^3)^{1481} \times 7 \equiv (1^3)^{1481} \times 7 \equiv 7$ [9]. Finalement, $1 \leqslant \sigma(B) \leqslant 12$ et $\sigma(B) \equiv 7$ [9] ce qui impose

$$\boxed{\sigma(B) = 7.}$$

Exercice 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.

Exercice n° 8

1) Pour $1 \leqslant k \leqslant n$, $k\binom{n}{k} = n\binom{n-1}{k-1}$. Donc, si k et n sont premiers entre eux, puisque n divise $k\binom{n}{k}$, le théorème de Gauss permet d'affirmer que n divise $\binom{n}{k}$.

2) De même, $(n+1)\binom{2n}{n-1} = n\binom{2n}{n}$ montre que $(n+1)$ divise $n\binom{2n}{n}$ et, puisque n et $(n+1)$ sont premiers entre eux (d'après Bezout puisque $(n+1)-n = 1$), $(n+1)$ divise $\binom{2n}{n}$ d'après le théorème de Gauss.

Exercice n° 9

1) Posons $d = \text{PGCD}(x, y)$ et $m = \text{PPCM}(x, y)$. 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 $\text{PGCD}(105, 56) = 7$ 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 $xy = 7 \times 105 = 735$. 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 $\text{PPCM}(21, 35) = 3 \times 5 \times 7 = 105$. Donc

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

2) On pose $x = dx'$ et $y = dy'$ avec x' et y' premiers entre eux et $d = \text{PGCD}(x, y)$. 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. $72 = 2^3 \times 3^2$ 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 $d = \dfrac{72}{1 \times 2} = 36$ puis $y = 36 \times 1 = 36$ et $x = y + d = 72$. Réciproquement, $72 - 36 = 36 = \text{PGCD}(36, 72)$ et $\text{PPCM}(36, 72) = 72$.
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.

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

3) Posons $d = \text{PGCD}(x, y)$ et $m = \text{PPCM}(x, y)$. d divise m et donc d divise $m - d = 243 = 3^5$ puis $d \in \{1, 3, 9, 27, 81, 243\}$.
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 $x'y' = 244 = 2^2 \times 61$ 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 $3x'y' - 3 = 243$ puis $x'y' = 81 + 1 = 82 = 2 \times 41$ 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 $x'y' = 27 + 1 = 28 = 2^2 \times 7$ 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 $x'y' = 9 + 1 = 10 = 2 \times 5$ 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 $x'y' = 3 + 1 = 4 = 2^2$ 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.

Exercice 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 $1 + 5\mathbb{Z}$ 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.

Exercice n° 11

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

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

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

$$F_m = q \times F_n + 1 + 1 = q \times F_n + 2,$$

où q est un entier.

Le PGCD 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 PGCD vaut donc 1 (ce résultat redémontre aussi l'existence d'une infinité de nombres premiers).

Exercice n° 12

1) Pour n entier naturel non nul donné, posons $v_n = u_{n+1}u_{n-1} - u_n^2$. 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 $\left((-1)^n u_{n-1}\right) u_{n+1} + \left((-1)^{n+1} u_n\right) u_n = 1$ 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 :

$$u_{n+m} = u_{n+1} = u_{n+1} \times 1 + u_n \times 0 = u_{n+1}u_1 + u_n u_0 = u_{n+1}u_m + u_{m-1}u_n.$$

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 $m \geqslant 1$. 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 non nuls tels que $n \geqslant m$. La division euclidienne de n par m s'écrit $n = mq + r$ avec q et r entiers tels que $0 \leqslant r \leqslant m-1$.
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 :

$$\text{PGCD}\left(u_m, u_r\right) = \text{PGCD}\left(u_m, u_{m+r}\right).$$

Puis, par récurrence

$$\text{PGCD}\left(u_m, u_r\right) = \text{PGCD}\left(u_m, u_{m+r}\right) = \text{PGCD}\left(u_m, u_{m+2r}\right) = \ldots = \text{PGCD}\left(u_m, u_{qm+r}\right) = \text{PGCD}\left(u_m, u_n\right).$$

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, $\text{PGCD}\left(u_m, u_n\right) = u_{\text{PGCD}(m,n)}$.

Exercice n° 13

1) Posons $d = \text{PGCD}(x, y, z)$ puis $x = dx'$, $y = dy'$ et $z = dz'$ où $\text{PGCD}(x', y', z') = 1$.

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

avec $\text{PGCD}(x', y', z') = 1$, 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, quite à permuter les lettres x et y, que x est impair et y est pair.

Posons alors $y = 2y'$ puis $X = \dfrac{z+x}{2}$ et $Z = \dfrac{z-x}{2}$ (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, $y = 2uv$ quite 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 $x = d\left(u^2 - v^2\right)$, $y = 2duv$ et $z = d\left(u^2 + v^2\right)$ ou bien $x = 2duv$, $y = d\left(u^2 - v^2\right)$ et $z = d\left(u^2 + v^2\right)$.

Réciproquement,

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

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 $(5,12,13)$.

Exercice n° 14

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

$$y\leqslant\sqrt[3]{\frac{349}{4}}=4,4...$$

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

$$x\leqslant\sqrt[3]{\frac{349}{3}}=4,8...$$

Donc, $x\in\{0,1,2,3,4\}$ ce qui ne laisse plus que $5\times5=25$ 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.

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

Exercice n° 15

Si $x\geqslant5$ et $5\leqslant k\leqslant x$, alors $k!$ est divisible par $2\times5=10$ puis $\displaystyle\sum_{k=5}^{x}k!$ est divisible par 10. D'autre part, $1!+2!+3!+4!=33$ et le chiffre des unités de $\displaystyle\sum_{k=1}^{x}k!$ est 3. $\displaystyle\sum_{k=1}^{x}k!$ 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, $x\leqslant4$. 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.

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

Exercice n° 16

$$\begin{aligned}n&=9+8(10+10^2+...+10^{p-1})+4(10^p+...+10^{2p-1})=9+80\frac{10^{p-1}-1}{10-1}+4\times10^p\frac{10^p-1}{10-1}\\&=\frac{1}{9}\left(81+80\left(10^{p-1}-1\right)+4\times10^p\left(10^p-1\right)\right)=\frac{1}{9}(4\times10^{2p}+4\times10^p+1)=\left(\frac{2\times10^p+1}{3}\right)^2,\end{aligned}$$

(ce qui montre déjà que n est le carré d'un rationnel). Maintenant, modulo 3,

$$2\times10^p+1\equiv2\times1^p+1\equiv0,$$

et $2\times10^p+1$ est un entier divisible par 3 ou encore $\dfrac{2\times10^p+1}{3}$ est un entier. Finalement, $n=\left(\dfrac{2.10^p+1}{3}\right)^2$ est bien le carré d'un entier.

Exercice n° 17

Pour $k\in\mathbb{N}$, posons $a_k=11...1$ ($k+1$ chiffres 1 en base 10).
Soit n un entier naturel quelconque.

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

Les $n+1$ entiers r_0, ... , 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 (principe des tiroirs). Par suite,

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

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

Exercice n° 18

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

2)

$$\begin{aligned}u_n^3&=\left(2^{n+1}+1\right)^3=2^{3n+3}+3\times 2^{2n+2}+3\times 2^{n+1}+1=2^{3n+3}+(2+1)\times 2^{2n+2}+(2+1)\times 2^{n+1}+1\\&=2^{3n+3}+2^{2n+3}+2^{2n+2}+2^{n+2}+2^{n+1}+1=10...0110...0110...01_2\end{aligned}$$

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

3)

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

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

Exercice n° 19

1) Soit $n\in\mathbb{N}^*$. Posons $n=\displaystyle\sum_{k=0}^{p}c_k10^k$, où $p\in\mathbb{N}$, et $\forall k\in[\![0,p]\!]$, $c_k\in[\![0,9]\!]$, et $c_p\neq 0$. Le nombre de chiffres de n est alors $p+1$. L'entier p vérifie $10^p\leqslant n<10^{p+1}$ ou encore $p\leqslant\log n<p+1$. Par suite, $p=\lfloor\log n\rfloor$. Ainsi,

$$\boxed{\text{le nombre de chiffres de } n \text{ en base 10 est } \lfloor\log n\rfloor+1.}$$

2) Pour $n\in\mathbb{N}^*$, posons $u_n=\dfrac{\sigma(n+1)}{\sigma(n)}$

a) Soit $n\in\mathbb{N}^*$. Posons $n=c_p10^p+...+10c_1+c_0=\overline{c_p...c_1c_0}_{10}$. 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, $0\leqslant k\leqslant p-1$ et $n=\overline{a_p...a_k9...9}_{10}$ et $n+1=\overline{a_p...a_{k+1}(a_k+1)0...0}_{10}$. Dans ce cas, si $k=0$,

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

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

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

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

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

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

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

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

$$\boxed{\text{La suite } u \text{ est bornée et diverge.}}$$

b) Avec les notations du a), $1 \leqslant \sigma(n) \leqslant 9(p+1) = 9(\lfloor \log n \rfloor + 1) \leqslant 9(\log n + 1)$.

c) Soit $n \in \mathbb{N}^*$. $1 \leqslant \sqrt[n]{\sigma(n)} \leqslant \sqrt[n]{9(\log n + 1)} = \exp\left(\dfrac{1}{n}\left(\ln 9 + \ln\left(1 + \dfrac{\ln n}{\ln 10}\right)\right)\right)$. Les deux membres de cet encadrement tendent vers 1 et donc la suite $\left(\sqrt[n]{\sigma(n)}\right)_{n\geqslant 1}$ converge et $\lim\limits_{n\to+\infty} \sqrt[n]{\sigma(n)} = 1$.

Exercice n° 20

1) (Formule de Legendre) Soit n un entier naturel supérieur ou égal à 2.
Si p est un nombre premier qui divise $n! = 1 \times 2 \ldots \times n$, alors p est un facteur premier de l'un des entiers 2,..., n et en particulier, $p \leqslant n$. Réciproquement, il est clair que si p est un nombre premier tel que $p \leqslant n$, 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 $p \leqslant n$. Pour trouver la valuation p-adique 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... et on s'arrête quand l'exposant k vérifie $p^k > n$. Or

$$n \geqslant p^k \Leftrightarrow \ln n \geqslant k \ln p \Leftrightarrow k \leqslant \frac{\ln n}{\ln p},$$

(car $\ln p > 0$). Donc, si $k \geqslant \left\lfloor \dfrac{\ln n}{\ln p} \right\rfloor + 1$, 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 multiple de p^3 inférieurs ou égaux à n... et du nombre de multiples de $p^{\lfloor \ln n / \ln p \rfloor}$ inférieurs ou égaux à n.

Soit k un entier tel que $1 \leqslant k \leqslant \left\lfloor \dfrac{\ln n}{\ln p} \right\rfloor$ et K un entier naturel.

$$1 \leqslant K \times p^k \leqslant n \Leftrightarrow \frac{1}{p^k} \leqslant K \leqslant \frac{n}{p^k} \Leftrightarrow 1 \leqslant K \leqslant \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Il y a donc $\left\lfloor \dfrac{n}{p^k} \right\rfloor$ multiples de p^k compris au sens large entre 1 et n. On a montré que la valuation p-adique de $n!$ est

$$\boxed{v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots}$$

2) Tout d'abord $10 = 2 \times 5$. L'exposant de 5 dans la décomposition primaire de 1000! est

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

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.

Exercice n° 21

Soit p un nombre premier.

1) Soit p un nombre premier et k un entier tel que $1 \leqslant k \leqslant p-1$. On a $k\dbinom{p}{k} = p\dbinom{p-1}{k-1}$. Donc, p divise $k\dbinom{p}{k}$. 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 $\dbinom{p}{k}$.

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

- C'est clair pour $a = 1$.
- Soit $a \geqslant 1$. Supposons que $a^p \equiv a\ (p)$. On a alors

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

On a montré par récurrence que

$$\boxed{\forall a \in \mathbb{N}^*,\ a^p \equiv a\ (p).}$$

Exercice n° 22

Soit p un entier naturel supérieur ou égal à 2.

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

Soit $k \in [\![1, p-1]\!]$. 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 $[\![1, p-1]\!]$ et donc, p est un nombre premier.

