ARITHMÉTIQUE DANS $\mathbb{Z}$

▶ Divisibilité, PGCD, PPCM

1. *Enoncé : Déterminer le pgcd et une relation de Bézout associés aux entiers 155 et 94 .*

$$\begin{array}{ll} 155 = 1 \times 94 + 61 & 1 = 3 - 2 \\ 94 = 1 \times 61 + 33 & 1 = 3 - (5 - 3) = 2 \times 3 - 5 \\ 61 = 1 \times 33 + 28 & 1 = 2 \times (28 - 5 \times 5) - 5 = 2 \times 28 - 11 \times 5 \\ 33 = 1 \times 28 + 5 & 1 = 2 \times 28 - 11 \times (33 - 28) = 13 \times 28 - 11 \times 33 \\ 28 = 5 \times 5 + 3 & 1 = 13 \times (61 - 33) - 11 \times 33 = 13 \times 61 - 24 \times 33 \\ 5 = 1 \times 3 + 2 & 1 = 13 \times 61 - 24 \times (94 - 61) = 37 \times 61 - 24 \times 94 \\ 3 = 1 \times 2 + 1 & 1 = 37 \times (155 - 94) - 24 \times 94 = 37 \times 155 - 61 \times 94 \end{array}$$

$$\text{Donc, } 155 \wedge 94 = 1 \quad \text{et} \quad 155 \wedge 94 = 37 \times 155 - 61 \times 94$$

2. *Enoncé : Soient $n, p \in \mathbb{Z}$. Montrer que :*

$$\Big(7 \mid x^2 + y^2\Big) \Longleftrightarrow (7 \mid x \text{ et } 7 \mid y).$$

Soit $x, y \in \mathbb{Z}$

$\underline{\Rightarrow :}$

Supposons que $7 \mid x^2 + y^2$.

$n \bmod 7$	$n^2 \bmod 7$
0	0
1	1
2	$4 \equiv -3$
3	2
4	$2 \equiv -3$
5	$4 \equiv -3$
6	1

Il n'y a aucune somme nulle entre deux termes, donc pour avoir $x^2 + y^2 \equiv 0 \pmod 7$, il faut que $x^2 \equiv 0$ et $y^2 \equiv 0$, donc $7 \mid x$ et $7 \mid y$.

$\underline{\Leftarrow :}$

Supposons que $7 \mid x$ et $7 \mid y$.

Donc on a $7 \mid x^2$ et $7 \mid y^2$, donc $7 \mid x^2 + y^2$.

3. *Enoncé : Résoudre les systèmes suivants :*

(a) $\begin{cases} x \wedge y = 3 \\ x \vee y = 135 \end{cases}$; (E)

Donc $\exists x', y' \in \mathbb{N}$ tels que $\begin{cases} x = 3x' \\ y = 3y' \end{cases}$

Donc, on a : $\begin{cases} x' \wedge y' = 1 \\ x' \vee y' = \frac{135}{3} = 45 \end{cases}$ (E').

Or $45 = 3^2 \times 5$,

Donc les solutions du système (E') sont $(9, 5)$ et $(5, 9)$.

Donc les solutions du système (E) sont $(27, 15)$ et $(15, 27)$.

(b) $\begin{cases} x+y=100 \\ x \wedge y = 10 \end{cases}$. (E)

Donc $\exists x', y' \in \mathbb{N}$ tels que $\begin{cases} x = 10x' \\ y = 10y' \end{cases}$

Donc on a : $\begin{cases} x'+y'=10 \\ x' \wedge y' = 1 \end{cases}$ (E').

On cherche les entiers naturels tel que les solutions de (E') avec un tableau.

x'	y'	$x' \wedge y'$
0	10	10
1	9	1
2	8	2
3	7	1
4	6	2
5	5	5

Les rôles de x' et y' sont interchangeables, donc les solutions du système (E') sont $(1,9)$ et $(9,1)$ et $(3,7)$ et $(7,3)$.

Donc les solutions du système (E) sont $(10,90)$ et $(90,10)$ et $(30,70)$ et $(70,30)$.

4. *Enoncé : Déterminer le reste de la division euclidienne de* 5^{2021} *par 3.*

On a :

$$5 \equiv 2 \pmod 3$$

Donc :

$$5 \times 5 \equiv 2 \times 2 \equiv 1 \pmod 3$$

Donc :

$$5^2 \equiv 1 \pmod 3$$

Or $2021 = 2 \times 1012 + 1$, donc :

$$5^{2021} = (5^2)^{1012} \times 5 \equiv 1^{1012} \times 2 \equiv 2 \pmod 3$$

Donc $\exists k \in \mathbb{Z}$ tel que $5^{2021} = 3k + 2$.

Comme $0 \leq 2 < 3$, alors par unicité de la division euclidienne, le reste est 2.

5. *Enoncé : Soient* $a, b \in \mathbb{Z}$ *tel que* $b \neq 0$. *Démontrer que :*

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$$

Par définition, on a :

$$a \vee b = \min\left((a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^*\right)$$

Soit $\mu \in \mathbb{N}$

Alors :

$$\mu = a \vee b \iff \begin{cases} \mu \in a\mathbb{Z} \cap b\mathbb{Z} \\ \forall m \in \mathbb{Z}, (m \in a\mathbb{Z} \cap b\mathbb{Z} \implies m \in \mu\mathbb{Z}) \end{cases} \iff \begin{cases} \mu \geq 0 \\ \mu\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} \end{cases}$$

6. *Enoncé : On considère la suite (* F_n *) définie par ses premiers termes* $\mathrm{F}_0 = 0$ *et* $\mathrm{F}_1 = 1$ *et par la relation de récurrence* $\mathrm{F}_{n+2} = \mathrm{F}_n + \mathrm{F}_{n+1}$ *pour* $n \in \mathbb{N}$.

(a) *Montrer que pour tout entier* $n \in \mathbb{N}^*$, $\mathrm{F}_{n-1}\,\mathrm{F}_{n+1} - \mathrm{F}_n^2 = (-1)^n$. *Déterminer le pgcd de* F_n *et* F_{n-1}.

On raisonne par récurrence.

Initialisation On a $\mathrm{F}_0\,\mathrm{F}_2 - \mathrm{F}_1^2 = -1 = (-1)^1$ donc la formule est vraie au rang 1.

Hérédité Supposons que $\mathrm{F}_{n-1}\,\mathrm{F}_{n+1} - \mathrm{F}_n^2 = (-1)^n$ pour un certain $n \in \mathbb{N}^*$.

$$\begin{aligned}\mathrm{F}_n\,\mathrm{F}_{n+2} - \mathrm{F}_{n+1}^2 &= \mathrm{F}_n(\,\mathrm{F}_{n+1} + \mathrm{F}_n) - \mathrm{F}_{n+1}(\,\mathrm{F}_{n-1} + \mathrm{F}_n)\\ &= \mathrm{F}_n^2 - \mathrm{F}_{n+1}\,\mathrm{F}_{n-1} = -(-1)^n = (-1)^{n+1}\end{aligned}$$

La formule est donc également vraie au rang $n+1$.

Conclusion La formule est vraie pour tout $n \in \mathbb{N}^*$.

On a donc une relation de Bézout entre F_n et F_{n-1} : ces deux entiers sont donc premiers entre eux.

(b) *Montrer que pour tout couple* $(n,p) \in \mathbb{N} \times \mathbb{N}^*$,

$$\mathrm{F}_{n+p} = \mathrm{F}_p\,\mathrm{F}_{n+1} + \mathrm{F}_{p-1}\,\mathrm{F}_n.$$

En déduire que $\mathrm{F}_n \wedge \mathrm{F}_p = \mathrm{F}_{n+p} \wedge \mathrm{F}_p$.

On raisonne par récurrence sur n (et pas sur p). L'hypothèse de récurrence au rang $n \in \mathbb{N}$ est la suivante : (H_n) : Pour tout $p \in \mathbb{N}^*$, $\mathrm{F}_{n+p} = \mathrm{F}_p\,\mathrm{F}_{n+1} + \mathrm{F}_{p-1}\,\mathrm{F}_n$.

Initialisation On a pour tout $p \in \mathbb{N}^*$:

$$\mathrm{F}_p\,\mathrm{F}_1 + \mathrm{F}_{p-1}\,\mathrm{F}_0 = \mathrm{F}_p$$

donc (H_0) est vraie.

Hérédité Supposons (H_n) pour un certain $n \in \mathbb{N}$. Soit $p \in \mathbb{N}^*$. Remarquons que $\mathrm{F}_{(n+1)+p} = \mathrm{F}_{n+(p+1)}$. Or $p+1 \in \mathbb{N}^*$. On applique notre hypothèse de récurrence (H_n) :

$$\begin{aligned}\mathrm{F}_{n+(p+1)} &= \mathrm{F}_{p+1}\,\mathrm{F}_{n+1} + \mathrm{F}_p\,\mathrm{F}_n\\ &= (\mathrm{F}_p + \mathrm{F}_{p-1})\,\mathrm{F}_{n+1} + \mathrm{F}_p\,\mathrm{F}_n\\ &= \mathrm{F}_p(\,\mathrm{F}_{n+1} + \mathrm{F}_n) + \mathrm{F}_{p-1}\,\mathrm{F}_{n+1}\\ &= \mathrm{F}_p\,\mathrm{F}_{n+2} + \mathrm{F}_{p-1}\,\mathrm{F}_{n+1}\end{aligned}$$

Ceci étant vrai quelque soit le choix de p, on en déduit que (H_{n+1}) est vraie.

Conclusion Pour tout $n \in \mathbb{N}, (\mathrm{H}_n)$ est vraie.

Soit $(n,p) \in \mathbb{N} \times \mathbb{N}^*$.

- Soit d un diviseur comun de F_n et F_p. Comme $\mathrm{F}_{n+p} = \mathrm{F}_p\,\mathrm{F}_{n+1} + \mathrm{F}_{p-1}\,\mathrm{F}_n$, d divise également F_{n+p}. Donc d est un diviseur commun de F_p et F_{n+p}.
- Réciproquement, soit d un diviseur commun de F_p et F_{n+p}. On en déduit que d divise $\mathrm{F}_{p-1}\,\mathrm{F}_n$ Or F_p et F_{p-1} sont premiers entre eux et d divise F_p, donc d et F_{p-1} sont également premiers entre eux. D'après le théorème de Gauss, d divise F_n. C'est donc un diviseur commun de F_n et F_p.

  On en conclut que $\mathrm{F}_n \wedge \mathrm{F}_p = \mathrm{F}_{n+p} \wedge \mathrm{F}_p$.
- *Démontrer que pour tout* $(m,n) \in \mathbb{N}^2$, $\mathrm{F}_m \wedge \mathrm{F}_n = \mathrm{F}_{m\wedge n}$.

  Soit $(m,n) \in \mathbb{N}^2$. On effectue la division euclidienne de m par n : $m = nq + r$.

  En itérant le résultat de la question précédente, on a

$$\mathrm{F}_n \wedge \mathrm{F}_r = \mathrm{F}_n \wedge \mathrm{F}_{r+n} = \mathrm{F}_n \wedge \mathrm{F}_{r+2n} = \cdots = \mathrm{F}_n \wedge \mathrm{F}_{r+nq} = \mathrm{F}_n \wedge \mathrm{F}_m$$

On conclut grâce à l'algorithme d'Euclide. Soit $d = m \wedge n$. Notons $a_0, \ldots, a_m = d$ la suite des restes non nuls obtenus par l'algorithme d'Euclide. D'après ce qui précéde,

$$\mathrm{F}_m \wedge \mathrm{F}_n = \mathrm{F}_n \wedge \mathrm{F}_{a_0} = \mathrm{F}_{a_0} \wedge \mathrm{F}_{a_1} = \cdots = \mathrm{F}_{a_m} \wedge \mathrm{F}_0 = \mathrm{F}_d$$

7. *Enoncé : Déterminer tous les entiers $n \in \mathbb{Z}$ tels que $n+1$ divise n^2+1.*

   Analyse :

   Soit $n \in \mathbb{Z}$ tel que $n+1 \mid n^2+1$.

   Alors :

   $$\begin{aligned} &n+1 \mid n^2+1 \\ &n+1 \mid (n+1)^2 - (n^2+1) \text{ car } n+1 \mid (n+1)^2 \\ &n+1 \mid 2n \end{aligned}$$

   De plus :

   $$n \times (-1) + (n+1) \times 1 = 1$$

   Donc par bézout, $n \wedge n+1 = 1$

   Donc par lemme de Gauss, $n+1|2$.

   Donc $n+1 \in \{-1, 1, -2, 2\}$ (diviseur de 2).

   Donc en réalisant un tableau :

$n+1$	n	n^2+1	Synthèse :
-2	-3	10	ok car $-2 \mid 10$
-1	-2	0	ok car $-1 \mid 5$
1	0	2	ok car $1 \mid 1$
2	1	2	ok car $2 \mid 2$

   Donc les solutions sont $n \in \{-3, -2, 0, 1\}$.

8. *Enoncé : Montrer que la plus grande puissance de 2 divisant $5^{2^n} - 1$ est 2^{n+2}.*

   Raisonnons par récurrence sur n.

   La propriété est évidente au rang $n = 0$. Supposons-la vraie à un certain rang $n \in \mathbb{N}$. Remarquons que

   $$5^{2^{n+1}} - 1 = \left(5^{2^n}\right)^2 - 1 = \left(5^{2^n} - 1\right)\left(5^{2^n} + 1\right)$$

   D'après l'hypothèse de récurrence 2^{n+2} est la plus grand puissance de 2 divisant $5^{2^n} - 1$. Montrons que 2 est la plus grande puissance de 2 divisant $5^{2^n} + 1$. On sait que $5 \equiv 1$ [4]. Donc $5^{2^n} + 1 \equiv 2$ [4]. Ceci prouve que 2 divise $5^{2^n} + 1$ mais que 4 ne le divise pas. En conclusion, 2^{n+3} est la plus grande puissance de 2 divisant $5^{2^{n+1}} - 1$.

▶ Entiers premiers entre eux

9. *Enoncé : Déterminer les entiers $x, y \in \mathbb{Z}$ tels que $5x^2 + 2xy - 3 = 0$.*
   On cherche les solutions de l'équation $5x^2 + 2xy - 3 = 0$. avec $x, y \in \mathbb{Z}$.

$$\begin{aligned} 5x^2 + 2xy - 3 &= 0 \\ 5x^2 + 2xy &= 3 \\ x(5x + 2y) &= 3 \end{aligned}$$

   Donc $x \mid 3$
   Or les diviseurs de 3 sont $\{-3, -1, 1, 3\}$.
   Donc $x \in \{-3, -1, 1, 3\}$ et on a :

x	$2x + 2y$	$2y$	y
-3	-1	14	7
-1	-3	2	1
1	3	-2	-1
3	1	-14	-7

   Donc d'après le tableau, les solutions sont $(x, y) \in \{(-3, 7), (-1, 1), (1, -1), (3, -7)\}$.

10. *Enoncé : Soit $n \in \mathbb{Z}$; démontrer que les entiers $20n^2 + 4n + 5$ et $10n^2 + 2n + 2$ sont premiers entre eux.*
    On a :

$$20n^2 + 4n + 5 = 2(10n^2 + 2n + 2) + 1$$

    Donc $20n^2 + 4n + 5$ et $10n^2 + 2n + 2$ sont premiers entre eux.

11. *Enoncé : Résoudre les équations diophantiennes suivantes :*
    (a) $15x + 6y = 3$;
    Posons l'équation :

$$15x + 6y = 3 \quad (\varepsilon)$$

    On a :

$$15 \wedge 6 = 3$$

    Donc $5x + 2y = 1$, or $5 \wedge 2 = 1$.
    Donc par bézout :

$$\exists u, v \in \mathbb{Z} \text{ tels que } 5u + 2v = 1$$

    On en déduit que $u = 1$ et $v = -2$.
    Donc $x_0 = 1$ et $y_0 = -2$. et $(x_0, y_0) = (1, -2)$ est une solution particulière de l'équation (ε).
    On a donc :

$$\begin{cases} 5x + 2y = 1 \\ 5x_0 + 2y_0 = 1 \end{cases}$$

    Donc :

$$5(x - x_0) = 2(y_0 - y)$$

    Donc $2 | 5(x - x_0)$, or $2 \wedge 5 = 1$.

Donc par gauss, $2 \mid (x - x_0)$ et on a :

$$\exists k \in \mathbb{Z} \text{ tels que } x = 2k + x_0$$

Donc on a :

$$\begin{aligned} 5(x - x_0) &= 2(y_0 - y) \\ 5(2k + x_0 - x_0) &= 2(y_0 - y) \\ 10k &= 2(y_0 - y) \\ 2y_0 - 10k &= 2y \\ y &= y_0 - 5k \end{aligned}$$

Vérification :

$$5(2k + 1) + 2(-5k - 2) = 10k + 5 - 10k - 4 = 1$$

Donc les solutions de l'équation (ε) sont :

$$(x, y) = (2k + 1, -5k - 2) \text{ pour } k \in \mathbb{Z}$$

(b) $42x + 28y = 14$;
Posons l'équation :

$$42x + 28y = 14 \quad (\varepsilon)$$

En simplifiant par 14, on a :

$$3x + 2y = 1$$

Donc, on a $x_0 = 1$ et $y_0 = -1$ et $(x_0, y_0) = (1, -1)$ est une solution particulière de l'équation (ε).
On a donc :

$$\begin{cases} 3x + 2y = 1 \\ 3x_0 + 2y_0 = 1 \end{cases}$$

Donc :

$$3(x - x_0) = 2(y_0 - y)$$

Donc $2|3(x - x_0)$, or $2 \wedge 3 = 1$.
Donc par gauss, $2 \mid (x - x_0)$ et on a :

$$\exists k \in \mathbb{Z} \text{ tels que } x = 2k + x_0$$

Donc on a :

$$\begin{aligned} 3(x - x_0) &= 2(y_0 - y) \\ 3(2k + x_0 - x_0) &= 2(y_0 - y) \\ 6k &= 2(y_0 - y) \\ 2y_0 - 6k &= 2y \\ y &= y_0 - 3k \end{aligned}$$

Vérification :

$$3(2k+1)+2(-3k-1)=6k+3-6k-2=1$$

Donc les solutions de l'équation (ε) sont :

$$(x,y)=(2k+1,-3k-1) \text{ pour } k\in\mathbb{Z}$$

(c) $9x+270y=7$.

Posons l'équation :

$$9x+270y=7 \quad (\varepsilon)$$

On a :

$$9\wedge 270=9$$

Donc $x+30y=\frac{7}{9}$, or $\frac{7}{9}\notin\mathbb{Z}$.

Donc l'équation (ε) n'a pas de solution dans $\mathbb{Z}$.

12. *Enoncé : Soit $n\in\mathbb{N}$. La fraction rationnelle $\frac{21n+4}{14n+3}$ est-elle irréductible ?*

Supposons que la fraction $\frac{21n+4}{14n+3}$ est réductible.

Alors il existe $d\in\mathbb{N}^*$ tel que $d\mid(21n+4)$ et $d\mid(14n+3)$.

Donc $d\mid(21n+4)-(14n+3)=7n+1$.

Donc $d\mid(14n+3)-2(7n+1)=1$.

Donc $d=1$.

Donc $21n+4$ et $14n+3$ sont premiers entre eux.

Ce qui est absurde. Donc la fraction $\frac{21n+4}{14n+3}$ est irréductible.

Sinon : En remarquant que $(21n+4)\times -2+(14n+3)\times 3=1$, on en déduit que $21n+4$ et $14n+3$ sont premiers entre eux par le théorème de Bézout.

13. *Enoncé : L'équation $x^3+x^2+2x+1=0$ admet-elle des solutions rationnelles ?*

Analyse :

Soit $x\in\mathbb{Q}$ tel que $x^3+x^2+2x+1=0$.

Posons $x=\dfrac{p}{q}$ avec $\begin{cases}p\in\mathbb{Z},q\in\mathbb{N}^*\\ p\wedge q=1\end{cases}$

Alors on a :

$$\frac{p^3}{q^3}+\frac{p^2}{q^2}+\frac{2p}{q}+1=0$$

Donc :

$$p^3+p^2q+2pq^2+q^3=0$$

C'est à dire :

$$p^3=q\left(-p^2-2pq-q^2\right)$$

Donc :

$$\begin{cases}q\mid p^3 \quad q\mid(p\times p^2)\\ q\wedge p=1\end{cases}$$

Donc par le lemme de Gauss :

$$\begin{cases}q\mid p^2 \quad q\mid(p\times p)\\ q\wedge p=1\end{cases}$$

Donc $q \mid p$.

Donc $q = 1$.

Donc $p = \pm 1$ ce qui est absurde.

Donc l'équation n'as pas de solution rationnelle.

14. *Enoncé : Soient a et b deux entiers non nuls premiers entre eux.*

(a) *Déterminer le pgcd de $a+b$ et ab.*

Soit p premier tel que $\begin{cases} p \mid ab \\ p \mid a+b \end{cases}$

Donc :

$$\begin{cases} p \mid a \quad \text{ou} \quad p \mid b \\ p \mid a+b \end{cases}$$

Or ce 'ou' est exclusif car a et b sont premiers entre eux.

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

(b) *Démontrer que $a^2 \wedge b^2 = 1$ et exprimer les coefficients de Bézout de a^2 et b^2 en fonction de ceux de a et b.*

On a : $a \wedge b = 1$.

Donc :

$$\exists u, v \in \mathbb{Z} \text{ tels que } au + bv = 1$$

Et donc on a :

$$\begin{aligned} 1 &= 1^2 \\ &= (au+bv)^2 \\ &= a^2u^2 + 2abuv + b^2v^2 \\ &= a^2u^2 + b^2v^2 + 2abuv \\ &= a^2\left(u^2 + 2bu^2v\right) + b^2\left(v^2 + 2av^2u\right) \end{aligned}$$

Donc on a :

$$a^2 \wedge b^2 = 1$$

Et les coefficients de Bézout sont $u^2 + 2bu^2v$ et $v^2 + 2av^2u$.

15. *Enoncé : Soient $a, b \in \mathbb{Z}$ premiers entre eux. Montrer que $a \wedge bc = a \wedge c$ pour tout $c \in \mathbb{Z}$.*

Soit $a, b, c \in \mathbb{Z}$.

Montrons que $\forall d \in \mathbb{Z}$, on a : $(d \mid bc) \wedge (d \mid a) \iff (d \mid a) \wedge (d \mid c)$.

$\Rightarrow$:

Supposons que $d \mid bc$ et $d \mid a$.

Alors on a :

$$\begin{cases} d \mid a \quad \text{Donc} \quad \exists k \in \mathbb{Z} \text{ tel que } a = kd \\ a \wedge b = 1 \quad \text{Donc} \quad \exists u, v \in \mathbb{Z} \text{ tels que } au + bv = 1 \end{cases}$$

Donc :

$$1 = d(ku) + bv$$

Donc :

$$d \wedge b = 1$$

Donc $d \mid c$.

$\Leftarrow$:

Supposons que $d \mid a$ et $d \mid c$.

Alors on a :

$$\begin{cases} d \mid a \\ d \mid bc \quad \text{car} \quad d \mid c \end{cases}$$

Donc ok.

16. *Enoncé : Déterminer les entiers $x, y, z \in \mathbb{N}^*$ tels que $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$.*

Remarquons qu'aucun des entiers x, y, z ne peut être égal à 1 . De plus, on ne peut avoir $x > 3, y > 3$ et $z > 3$ car sinon $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} < 1$.

Donc l'un des trois entiers est inférieur ou égal à 3 . Supposons que ce soit x : on peut avoir $x = 2$ ou $x = 3$.

Cas $x = 2$: On a alors $\frac{1}{y} + \frac{1}{z} = \frac{1}{2}$. Comme auparavant, aucun des entiers y et z ne peut être égal à 2 et on ne peut avoir $y > 4$ et $z > 4$. L'un de ces deux entiers est donc inférieur ou égal à 4 . Supposons que ce soit y.

Cas $y = 3$: On obtient $z = 6$.

Cas $y = 4$: On obtient $z = 4$.

Cas $x = 3$: On a alors $\frac{1}{y} + \frac{1}{z} = \frac{2}{3}$. On ne peut avoir $y > 3$ et $z > 3$. L'un de ces deux entiers est donc inférieur ou égal à 3 . Supposons que ce soit y.

Cas $y = 2$: On obtient $z = 6$.

Cas $y = 3$: On obtient $z = 3$.

En conclusion, les solutions sont les triplets $(2, 3, 6), (2, 4, 4), (3, 3, 3)$ et toutes les permutations de ceux-ci.

▶ Nombres premiers

17. *Enoncé : Pour $n \geq 2$, on appelle n-ième nombre de Mersenne l'entier $M_n = 2^n - 1$.*

(a) *Démontrer que pour tout $n \geq 2$, si M_n est premier alors n l'est.*

Soit $n \geq 2$, $M_n = 2^n - 1$.

Par contraposée, supposons que n est composé.

C'est à dire :

$$\exists a, b \geq 2 \text{ tels que } n = ab$$

Donc on a :

$$\begin{aligned} M_n = 2^{ab} - 1^b &= (2^b)^a - 1^b \\ &= (2^a - 1) \sum_{k=0}^{b-1} 2^{ak} \end{aligned}$$

Donc M_n est composé.

(b) *Que dire de la réciproque ?*

La réciproque est fausse.

Contre-exemple : $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ est composé mais 11 est premier.

18. *Enoncé : Pour $n \in \mathbb{N}$ on note $D(n)$ la somme de tous les diviseurs strictement positifs de n et $\mathrm{Div}(n)$ l'ensemble de ces derniers.*

(a) *Calculer $D(n)$ pour n compris entre 1 et 17 .*
Soit $n \in \mathbb{N}$, alors notons $\mathrm{Div}(n) = \{d > 0 \mid d \mid n\}$ et $D(n) = \sum_{d \in \mathrm{Div}(n)} d$.

On a alors :

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$D(n)$	1	3	4	7	6	12	8	15	13	18	12	28	14	24	24	31	18

(b) *Déterminer $D(p^\alpha)$ pour p premier et $\alpha \geq 1$.*
Soit p un nombre premier et $\alpha \geq 1$. On a alors :

$$\mathrm{Div}(p^\alpha) = \{1, p, p^2, \ldots, p^\alpha\}$$

et donc :

$$D(p^\alpha) = \sum_{k=0}^{\alpha} p^k = \frac{p^{\alpha+1} - 1}{p - 1}.$$

(c) *Soient $a, b \in \mathbb{N}^*$ premiers entre eux. Démontrer que l'application*

$$\begin{aligned} \pi : \mathrm{Div}(a) \times \mathrm{Div}(b) &\to \mathrm{Div}(ab) \\ (d_1, d_2) &\mapsto d_1 d_2 \end{aligned}$$

est bijective. En déduire que $D(ab) = D(a)D(b)$.
Soit $a, b \in \mathbb{N}^*$ premiers entre eux.
Donc $a \wedge b = 1$
Posons l'application :

$$\begin{aligned} \pi : \mathrm{Div}(a) \times \mathrm{Div}(b) &\to \mathrm{Div}(ab) \\ (d_1, d_2) &\mapsto d_1 d_2 \end{aligned}$$

π est bien définis car si $u \mid a$, $v \mid b$ alors $uv \mid ab$.
Injectivité :
Soit $(u, v), (u', v') \in \mathrm{Div}(a) \times \mathrm{Div}(b)$ tels que $uv = u'v'$.
Donc

$$\begin{cases} u \mid u'v' \\ u \wedge v' = 1 \quad \text{car } a \wedge b = 1 \text{ et } u \mid a \text{ et } v' \mid b \end{cases}$$

Donc $u \mid u'$.
Donc $u' \mid u$.
Donc $u, v > 0$ et $\begin{cases} u = u' \\ v = v' \end{cases}$
Surjectivité :
Soit $d \in \mathrm{Div}(ab)$.
Par développement en produit de facteurs premiers, on a :

$$\exists p_1, p_2, \ldots, p_k \text{ premiers tels que } d = \prod_{k=1}^{n} p_i^{\alpha_i}$$

Donc $\forall i \in [\![1, k]\!]$, on a $p_i^{\alpha_i} \mid d.$ et $d \mid ab.$
Donc :

$$(p_i)^{\alpha_i} \mid ab$$

Donc on a :

$$(p_i)^{\alpha_i} \mid a \text{ ou } (p_i)^{\alpha_i} \mid b$$

Comme p_1 est premier, on a plus simplement :

$$p_1 \mid a \text{ ou } p_1 \mid b$$

Le ou est exclusif car a et b sont premiers entre eux.

(d) *Donner une méthode permettant, connaissant un entier n et sa décomposition en produit de facteurs premiers, de calculer $D(n)$. En déduire $D(2021)$.*
Posons $\text{Div}(a) = \{a_1, a_2, \dots, a_k\}$ et $\text{Div}(b) = \{b_1, b_2, \dots, b_l\}$.
Alors :

$$\begin{aligned}\text{Div}(ab) = \pi\left(\text{Div}(a) \times \text{Div}(b)\right) &= \{\pi(u, v) \mid u \in \text{Div}(a), v \in \text{Div}(b)\} \\ &= \{a_i b_j \mid i \in [\![1, k]\!], j \in [\![1, l]\!]\}\end{aligned}$$

Donc :

$$D(ab) = \sum_{i=1}^{k}\sum_{j=1}^{l} a_i b_j = \sum_{i=1}^{k} a_i \sum_{j=1}^{l} b_j = D(a)D(b)$$

Donc :

$$D(\prod_{i=1}^{n} p_i^{\alpha_i}) = \prod_{i=1}^{n} D(p_i^{\alpha_i}) = \prod_{i=1}^{n} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

(e) *Calculer $D(2021)$.*
On a la décomposition en facteurs premiers suivante :

$$2021 = 43 \times 47$$

Donc comme précédemment, on a :

$$\begin{aligned}D(2021) &= D(43)D(47) \\ &= \frac{43^{1+1} - 1}{43 - 1} \times \frac{47^{1+1} - 1}{47 - 1} \\ &= \frac{43^2 - 1}{42} \times \frac{47^2 - 1}{46} \\ &= \frac{1849 - 1}{42} \times \frac{2209 - 1}{46} \\ &= \frac{1848}{42} \times \frac{2208}{46} \\ &= 44 \times 48 \\ &= 2112\end{aligned}$$

▶ Approfondissement

19. *Enoncé : Montrer que pour tout $n \in \mathbb{N}^*$, on a :*

$$10^{10^n} \equiv 4\ [7].$$

Posons $\mathrm{A} = 10^{10^n}$. On a $\mathrm{A} \equiv 3^{10^n}[7]$ et, puisque 7 est un nombre premier ne divisant pas 3 , d'après le petit théorème de Fermat, $3^6 \equiv 1[7]$. Recherchons donc le reste de 10^n modulo 6 , c'est-à-dire le reste de 4^n modulo 6 . On obtient $4^2 \equiv 4[7]$, puis, pour tout entier $n \geq 2$,

$$4^n \equiv 4^2 4^{n-2} \equiv 4 \cdot 4^{n-2} \equiv 4^{n-1}[6]$$

On a donc, pour $n \geq 1, 4^n \equiv 4[6]$ et $A \equiv 3^4 = 81 \equiv 4[7]$.

20. *Enoncé : Formule de Legendre.*

(a) *Soient $n \in \mathbb{N}^*$ et $x \in \mathbb{R}$. Démontrer que :*

$$\left\lfloor \frac{\lfloor xn \rfloor}{n} \right\rfloor = \lfloor x \rfloor.$$

On a $\lfloor nx \rfloor \leq nx$ puis $\frac{\lfloor nx \rfloor}{n} \leq x$, or $x \mapsto \lfloor x \rfloor$ est croissante donc

$$\left\lfloor \frac{\lfloor nx \rfloor}{n} \right\rfloor \leq \lfloor x \rfloor$$

$$\lfloor x \rfloor \leq x \text{ donc } n\lfloor x \rfloor \leq nx \text{ puis } n\lfloor x \rfloor \leq \lfloor nx \rfloor \text{ car } n\lfloor x \rfloor \in \mathbb{Z}.$$

Par suite

$$\lfloor x \rfloor \leq \frac{\lfloor nx \rfloor}{n}$$

puis

$$\lfloor x \rfloor \leq \left\lfloor \frac{\lfloor nx \rfloor}{n} \right\rfloor$$

et finalement

$$\lfloor x \rfloor = \left\lfloor \frac{\lfloor nx \rfloor}{n} \right\rfloor$$

(b) *En déduire que si p est un nombre premier et $n \in \mathbb{N}$, alors :*

$$v_p(n!) = \sum_{i=0}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor, \quad \text{avec} \quad k = \left\lfloor \frac{\ln(n)}{\ln(p)} \right\rfloor.$$

En isolant les multiples de p dans le produit décrivant $p\,!$, on obtient

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + v_p\left(\left\lfloor \frac{n}{p} \right\rfloor ! \right)$$

puis

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{\lfloor n/p \rfloor}{p} \right\rfloor + v_p\left(\left\lfloor \frac{\lfloor n/p \rfloor}{p} \right\rfloor ! \right)$$

or

$$\left\lfloor \frac{\lfloor px \rfloor}{p} \right\rfloor = \lfloor x \rfloor$$

avec $x = n/p^2$ donne

$$\left\lfloor \frac{\lfloor n/p \rfloor}{p} \right\rfloor = \left\lfloor \frac{n}{p^2} \right\rfloor$$

puis finalement

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor$$

avec

$$k = \left\lfloor \frac{\ln n}{\ln p} \right\rfloor$$

21. *Enoncé : Montrer que si p est un entier premier différent de 2 et 5, alors il divise un des entiers de l'ensemble $\{1, 11, 111, 1111, \ldots\}$.*

    L'ensemble de l'énoncé est formé des entiers de la forme $u_n = \sum_{k=0}^{n} 10^k$ pour $n \in \mathbb{N}$. On a facilement $u_n = \frac{1}{9}(10^{n+1} - 1)$. Soit p un entier premier différent de 2,3 et 5 . Alors $10 = 2 \times 5$ est premier avec p. D'après le petit théorème de Fermat, $10^{p-1} \equiv 1[p]$ donc p divise $10^{p-1} - 1$. Comme $p \neq 3, p$ est premier avec 9 . On sait que 9 divise $10^{p-1} - 1$ puisque $\frac{1}{9}(10^{p-1} - 1) = u_{p-2} \in \mathbb{N}$. Donc $9p$ divise $10^{p-1} - 1$ i.e. p divise u_{p-2}.

22. *Enoncé : Montrer que la somme de deux nombres premiers consécutifs ne peut pas être égale au produit de deux nombres premiers.*

    Soient p et q deux nombres premiers consécutifs avec $p < q$.

    Si $p = 2$, alors $q = 3$ et $p + q = 5$ ne peut être le produit de deux nombres premiers.
    Si $p > 2$, alors p et q sont impairs donc $p + q$ est pair. Supposons qu'il existe deux nombres premiers a et b tels que $p+q = ab$. Comme $p+q$ est pair, un des deux nombres premiers a et b est égal à 2 par unicité de la décomposition en facteurs premiers. Supposons sans perte de généralité que $a = 2$. Alors $b = \frac{p+q}{2}$ est un nombre premier strictement compris entre p et q, ce qui contredit le fait que p et q sont des nombres premiers consécutifs.