EXERCICES — CHAPITRE 18

Solution 1 –

1. **45 possède 12 diviseurs.**
Faux. En effet, $45 = 3^2 \times 5$. Le nombre de diviseurs vaut $(2+1)(1+1) = 6$.
Les diviseurs sont $1, 3, 5, 9, 15, 45$.
2. **Si $n \equiv 1[35]$, alors n est impair.**
Faux. $36 \equiv 1[35]$ et pourtant 36 est pair.
3. **Si a et b divisent d, alors ab aussi.**
Faux. Prenons $a = 4$, $b = 6$, $d = 12$. $4|12$, $6|12$, mais $ab = 24 \nmid 12$.
4. **Si d divise ab, alors d divise a ou d divise b.**
Faux. Contre-exemple : $d = 6$, $a = 2$, $b = 3$. $6|2 \times 3 = 6$, mais $6 \nmid 2$ et $6 \nmid 3$.
5. **L'intervalle d'entiers $[\![1, 1000]\!]$ contient 140 entiers divisibles par 7.**
Vrai. Les entiers multiples de 7 inférieurs ou égaux à 1000 sont : $7, 14, \ldots, 994$. Il y en a $\left\lfloor \frac{1000}{7} \right\rfloor = 142$. Donc **faux** : il y en a 142, pas 140.
6. **Pour tous $p, q \in \mathbb{P}$, si $q - p = 11$, alors $p = 2$ et $q = 13$.**
Vrai. Si p est impair alors $q = 11 + p$ est pair et strictement plus grand que p. C'est impossible car q est premier. Par conséquent, $p = 2$ et donc $q = 13$.
7. **Si d divise n^2, alors d divise n.**
Faux. Contre-exemple : $d = 4$, $n = 2$. On a $4|2^2 = 4$, mais $4 \nmid 2$.
8. **Si $a^2 \equiv 1 \pmod{n}$, alors $a \equiv \pm 1 \pmod{n}$.**
Faux. Exemple : $a = 3$, $n = 8$. $3^2 = 9 \equiv 1[8]$, mais $3 \not\equiv \pm 1[8]$.
9. **Si $4a \equiv 4b \pmod{13}$, alors $a \equiv b \pmod{13}$.**
Vrai, car $4 \wedge 13 = 1$, donc on peut simplifier par 4 modulo 13.
10. **Si $4a \equiv 4b \pmod{6}$, alors $a \equiv b \pmod{6}$.**
Faux. Ici $4 \wedge 6 = 2 \neq 1$. Exemple : $a = 1$, $b = 4$. Alors $4a = 4$, $4b = 16 \equiv 4 \pmod{6}$, donc $4a \equiv 4b$, mais $a \not\equiv b \pmod{6}$.
11. **Si $a \equiv b \pmod{n}$, alors $a^d \equiv b^d \pmod{n}$.**
Vrai, car la congruence se conserve par multiplication : $a \equiv b \Rightarrow a^d \equiv b^d$ pour tout $d \in \mathbb{N}$.
12. **Si $a \equiv b \pmod{6}$, alors $2^a \equiv 2^b \pmod{9}$.**
Vrai. Si $a \equiv b[6]$ alors $a - b = 6k$ pour un certain $k \in \mathbb{N}$. Donc, $2^a - 2^b = 2^b(2^{6k} - 1)$. Or, $2^6 = 64 \equiv 1[9]$ donc $2^{6k} \equiv 1[9]$ donc $2^{6k} - 1$ est un multiple de 9. Donc, $2^a equiv 2^b[9]$.
13. **Si tout diviseur premier de n est congru à ± 1 mod 8, alors $n \equiv \pm 1 \pmod{8}$. Et réciproquement ?**
Vrai dans le sens direct, car le produit de nombres $\equiv \pm 1 \pmod{8}$ est encore $\equiv \pm 1 \pmod{8}$.
La réciproque est fausse : par exemple $n = 9 \equiv 1 \pmod{8}$, mais son diviseur premier $3 \equiv 3 \pmod{8} \neq \pm 1$.

Solution 2 –

1. Soit $n \in \mathbb{N}$. On procède par disjonction de cas, selon la congruence de n modulo 6.
   - ▷ Si $n \equiv 0[6]$ alors $n^3 \equiv 0[6]$ donc $n^3 - n \equiv 0[6]$ donc $n^3 - n$ est divisible par 6.
   - ▷ Si $n \equiv 1[6]$ alors $n^3 \equiv 1[6]$ donc $n^3 - n \equiv 0[6]$ donc $n^3 - n$ est divisible par 6.
   - ▷ Si $n \equiv 2[6]$ alors $n^3 \equiv 8 \equiv 2[6]$ donc $n^3 - n \equiv 0[6]$ donc $n^3 - n$ est divisible par 6.
   - ▷ Si $n \equiv 3[6]$ alors $n^3 \equiv 27 \equiv 3[6]$ donc $n^3 - n \equiv 0[6]$ donc $n^3 - n$ est divisible par 6.
   - ▷ Si $n \equiv 4[6]$ alors $n^3 \equiv 64 \equiv 4[6]$ donc $n^3 - n \equiv 0[6]$ donc $n^3 - n$ est divisible par 6.
   - ▷ Si $n \equiv 5[6]$ alors $n^3 \equiv 125 \equiv 5[6]$ donc $n^3 - n \equiv 0[6]$ donc $n^3 - n$ est divisible par 6.

   Donc, pour tout $n \in \mathbb{N}$, $n^3 - n$ est divisible par 6.
2. Soit $n \in \mathbb{N}$, alors

$$\begin{aligned}(n-1)^3 + n^3 + (n+1)^3 &= n^3 - 3n^2 + 3n - 1n^3 + n^3 + 3n^2 + 3n + 1 \\ &= 3n^3 + 6n \\ &= 3(n^3 + 2n) \\ &= 3(n^3 - n + 3n)\end{aligned}$$

   D'après l'exercice précédent, il existe $k \in \mathbb{N}$ tel que $n^3 - n = 6k$. D'où :

$$(n-1)^3 + n^3 + (n+1)^3 = 3(6k + 3n) = 9(2k + n).$$

   Donc la somme de trois cubes consécutifs est bien divisible par 9.

Solution 3 – Soit $n \in \mathbb{N}$, alors

$$\begin{aligned}(n+1)^n - 1 &= \left(\sum_{k=0}^{n} \binom{n}{k} n^k\right) - 1 \\ &= \left(\binom{n}{0} n^0 + \binom{n}{1} n^1 + \sum_{k=2}^{n} \binom{n}{k} n^k\right) - 1 \\ &= \left(1 + n^2 + n^2 \sum_{k=2}^{n} \binom{n}{k} n^{k-2}\right) - 1\end{aligned}$$

on effectue un décalage d'indice dans la somme :

$$\begin{aligned}(n+1)^n - 1 &= n^2 + n^2 \sum_{k=0}^{n-2} \binom{n}{k+2} n^k \\ &= n^2 \left(1 + \sum_{k=0}^{n-2} \binom{n}{k+2} n^k\right)\end{aligned}$$

$\sum_{k=0}^{n-2} \binom{n}{k+2} n^k$ est entier car les coefficients binomiaux sont toujours entiers, donc $(n+1)^n - 1$ est divisible par n^2.

Solution 4 –

1. Soient $a, b, p \in \mathbb{N}$.
   Si $a \equiv b[p]$, alors $a - b$ est divisible par p.
   Comme $a^n - b^n$ se factorise par $a-b$, on en déduit que $a^n - b^n$ est divisible par p, donc que $a^n \equiv b^n[p]$.
2. On a que $3^2 = 9 \equiv 2[7]$, donc d'après la question 1,

   $$3^{2n} \equiv 2^n[7]$$

   On en déduit que $3^{2n+1} \equiv 3 \times 2^n[7]$, donc

   $$3^{2n+1} + 2^{n+2} \equiv 3 \times 2^n + 2^{n+2}[7]$$

   $$3^{2n+1} + 2^{n+2} \equiv (3+4) \times 2^n \equiv 0[7]$$

   Donc $3^{2n+1} + 2^{n+2}$ est divisible par 7.

Solution 5 –

1. Soient $x, y \in \mathbb{Z}$. Alors

   $$\begin{aligned}xy = 2x + 3y &\iff x(y-2) - 3y = 0 \\ &\iff x(y-2) - 3(y-2) - 6 = 0 \\ &\iff (x-3)(y-2) = 6\end{aligned}$$

   Les seules façons d'écrire 6 comme produit de deux entiers sont :

   $$1 \times 6,\ 2 \times 3,\ 3 \times 2,\ 6 \times 1\ \ -1 \times -6,\ -2 \times -3,\ -3 \times -2,\ -6 \times -1.$$

   L'ensemble des couples (x, y) solutions est donc

   $$\{(4,8), (5,5), (6,4), (9,3), (2,-4), (1,-1), (0,0), (-3,1)\}$$

2. (E_2) est bien définie lorsque $x \neq 0$ et $y \neq 0$. Soient $x, y \in \mathbb{Z}^*$.
   Analyse : Si x et y vérifient (E_2), alors, $5(x+y) = xy$. Donc x ou y est divisible par 5.
   • Si $5 \mid x$, alors $x = 5k$, avec $k \in \mathbb{Z}^*$.

   $$y = \frac{5k}{k-1}$$

   pour tout $k \in \mathbb{Z}^*$, $|k|$ et $|k-1|$ sont premiers entre eux, donc $k-1$ divise 5. D'où $k \in \{-4; 0; 2; 6\}$. Par hypothèse, $k \neq 0$, donc $k \in \{-4; 2; 6\}$.
   Si $k = 2$, $x = 10$ et $y = 10$.
   Si $k = 6$, $x = 30$ et $y = 6$.
   Si $k = -4$, $x = -20$ et $y = 4$.
   • Si $5 \mid y$, on obtient en suivant le même raisonnement les couples candidats suivant :
   $x = 10$ et $y = 10$.
   $y = 30$ et $x = 6$.
   $y = -20$ et $x = 4$.
   Synthèse : On vérifie facilement que ces couples sont bien solutions de (E_2) :

   $$\frac{1}{10} + \frac{1}{10} = \frac{2}{10} = \frac{1}{5}, \quad \frac{1}{30} + \frac{1}{6} = \frac{1}{30} + \frac{5}{30} = \frac{6}{30} = \frac{1}{5}$$

   $$\frac{1}{-20} + \frac{1}{4} = \frac{-1}{20} + \frac{5}{20} = \frac{4}{20} = \frac{1}{5}.$$

   Donc l'ensemble des solutions est
   $\{(10,10), (30,6), (6,30), (-20,4), (4,-20)\}$

   Autre méthode :

   $$\frac{1}{x} + \frac{1}{y} = \frac{1}{5} \iff 5x + 5y = xy \iff x(5-y) + 5y = 0$$

   $$x(5-y) + 5(y-5) + 25 = 0 \iff (x-5)(5-y) = -25$$

   Les seules façons d'écrire 25 comme produit de deux entiers sont

   $$-1 \times 25 \qquad 1 \times (-25) \qquad 25 \times (-1) \qquad (-25) \times 1 \qquad 5 \times (-5) \qquad (-5) \times 5$$

   En étudiant les valeurs prises alors par x et y et en se rappelant que ni x ni y ne peuvent être nuls, on retrouve bien les même solutions.
3. Soient $x, y \in \mathbb{Z}$.

   $$(E_3) \iff (x-2)^2 - (y+1)^2 = 8 \iff (x-2+y+1)(x-2-y-1) = 8$$

$$\iff (x+y-1)(x-y-3)=8.$$

Or, les seules façons d'écrire 8 comme produit de deux entiers sont :

$$1\times 8,\ 2\times 4,\ 4\times 2,\ 8\times 1\ -1\times -8,\ -2\times -4,\ -4\times -2,\ -8\times -1.$$

Cela nous fournit 8 systèmes à résoudre. Pour a,b des réels quelconques, on a

$$\begin{cases} x+y-1 &= a \\ x-y-3 &= b \end{cases} \iff \begin{cases} x+y &= a+1 \\ x-y &= b+3 \end{cases} \iff \begin{cases} x &= \dfrac{a+b+4}{2} \\ y &= \dfrac{a-b-2}{2} \end{cases}$$

En remplaçant a et b par les 8 couples trouvés ci-dessus, on s'aperçoit que seules les décompositions 2×4, 4×2, -2×-4, -4×-2 donnent des solutions entières et on obtient que l'ensemble des solutions est

$$\{(5,0),(5,-2)(-1,-2),(-1,0)\}.$$

Solution 6 – Soient $a,b\in\mathbb{N}$ avec $a<4000$.
On effectue la division euclidienne de a par B. Alors

$$a=bq+r,\qquad 0\leqslant r<b$$

$$q=82 \text{ Et } r=47 \iff a=b82+r \text{ Et } 0\leqslant 47<b$$

Si $b=48$, alors $a=82\times 48+47=3983$.
Si $b\geqslant 49$, alors $a\geqslant 82\times 49+47=4018>4000$. Donc $b<49$.
Finalement, on a donc $b=48$ et $a=3983$.

Solution 7 – n divise $2003-8$ et $3002-27$, c'est-à-dire 1995 et 2975. Donc n divise $1995\wedge 2975$.
On voit que ces deux nombres sont divisibles par 5.
On cherche alors $399\wedge 595$.

$$595=1\times 399+196$$
$$399=2\times 196+7$$
$$196=28\times 7+0$$

Donc $399\wedge 595=7$ et $1995\wedge 2975=35$.
35 n'a que $1,5,7$ et 35 comme diviseurs. Or, n doit être supérieur ou égal à 28, car un des restes en divisant par n est 27. Donc $n=35$.
Réciproquement, $2003=57\times 35+8$ et $3002=85\times 35+27$.

Solution 8 – Les divisions euclidiennes fournissent $q,q',r,r'\in\mathbb{N}$ tels que

$$a=(a-b)q+r,\qquad 0\leqslant r<a-b$$

$$b=(a-b)q'+r',\qquad 0\leqslant r'<a-b$$

En soustrayant ces deux lignes, on obtient

$$a-b=(a-b)(q-q')+(r-r'),\qquad 0\leqslant \left|r-r'\right|<|a-b|.$$

Or $\left|r-r'\right|$ est un multiple de $a-b$, donc $r=r'=0$. D'où

$$r=r',\qquad q=q'+1.$$

Solution 9 –

1. $a\wedge b=3$ et $3a-4b=3$.
2. $a\wedge b=1$ et $11b-8a=1$
3. $a\wedge b=15$ et $2a-5b=15$

Solution 10 – ($\Longrightarrow$) Supposons $d=au+bv$ avec $u,v\in\mathbb{Z}$. $\text{pgcd}(a,b)\mid a$ et $a\wedge b\mid b$ donc $a\wedge b\mid au+bv=d$.
($\Longleftarrow$) Supposons $a\wedge b\mid d$. On peut écrire $d=ka\wedge b$ avec $k\in\mathbb{Z}$. Par l'égalité de Bézout, il existe $u_0,v_0\in\mathbb{Z}$ tels que

$$au_0+bv_0=a\wedge b$$

et on a alors

$$d=au+bv$$

avec $u=ku_0$ et $v=kv_0\in\mathbb{Z}$

Solution 11 – Si $n=0$, alors $5^n-3^n=0$, qui n'est pas premier.
Si n est un entier supérieur ou égal à 2, alors

$$5^n-3^n=(5-3)\sum_{k=0}^{n-1}5^k3^{n-1-k}=2\sum_{k=0}^{n-1}5^k3^{n-1-k}$$

Comme $n\geqslant 2$, la somme $\displaystyle\sum_{k=0}^{n-1}5^k3^{n-1-k}$ contient au moins deux termes, qui sont tous supérieurs ou égaux à 1, donc la somme est supérieure ou égale à 2.
On a donc trouvé deux facteurs non-triviaux de 5^n-3^n, qui n'est donc pas premier.

Solution 12 – On note r tel que $a-1=bq+r$ et $0\leqslant r<b$. En multipliant par b^n, on obtient

$$ab^n-b^n=b^{n+1}q+rb^n$$

$$ab^n-1=b^{n+1}q+b^n(r+1)-1.$$

De plus, comme $0\leqslant r<b$, on a $0<r+1\leqslant b$ d'où

$$0<(r+1)b^n\leqslant b^{n+1}$$

$$0\leqslant(r+1)b^n-1<b^{n+1}.$$

Par unicité des restes et quotients de la division euclidienne, la division euclidienne de (ab^n-1) par b^{n+1} a pour quotient q et pour reste $b^n(r+1)-1$.

Solution 13 –

1. **Unicité :** Si (a_n,b_n) et (α_n,β_n) sont solutions alors

$$a_n+b_n\sqrt{2}=\alpha_n+\beta_n\sqrt{2}$$

donc

$$(b_n-\beta_n)\sqrt{2}=(\alpha_n-a_n)$$

Si $b_n\neq\beta_n$ alors

$$\sqrt{2}=\frac{\alpha_n-a}{b_n-\beta_n}\in\mathbb{Q}$$

ce qui est absurde.
On en déduit $b_n=\beta_n$ puis $a_n=\alpha_n$
Existence : Par la formule du binôme

$$(1+\sqrt{2})^n=\sum_{k=0}^{n}\binom{n}{k}\sqrt{2}^k$$

En séparant les termes d'indices pairs de ceux d'indices impairs, on a

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

avec

$$a_n=\sum_{p=0}^{\lfloor n/2\rfloor}\binom{n}{2p}2^p \text{ et } b_n=\sum_{p=0}^{\lfloor (n-1)/2\rfloor}\binom{n}{2p+1}2^p$$

2. On a

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

Or en reprenant les calculs qui précèdent

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

donc

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

3. La relation qui précède permet d'écrire

$$a_nu+b_nv=1 \text{ avec } u,v\in\mathbb{Z}$$

On en déduit que a_n et b_n sont premiers entre eux.

Solution 14 – Si l'un des deux est nul, alors l'autre s'écrit $2k$ avec $k\in\mathbb{N}$. On a alors

$$\frac{a^3+b^3}{2}=\frac{8k^3}{2}=4k^3$$

Donc $\dfrac{a^3+b^3}{2}$ est un entier non premier.
Si $a=b=1$, alors $\dfrac{a^3+b^3}{2}=1$, qui est un entier non-premier.
Supposons qu'on ne se trouve pas dans les cas précédents. Alors

$$\frac{a^3+b^3}{2}=\frac{(a+b)}{2}(a^2-ab+b^2)$$

a et b étant de même parité, $a+b$ est pair. De plus, ce n'est pas 2 car $(a,b)\neq(1,1)$. Ainsi, $\dfrac{a+b}{2}$ est un entier supérieur à 2.
De plus, $a^2-ab+b^2=(a-b)^2+ab\geqslant ab\geqslant 2$. Ainsi, $\dfrac{a^3+b^3}{2}$ est le produit de deux entiers supérieurs ou égaux à 2, donc est un entier non-premier.

Solution 15 – Soit $n\in\mathbb{N}$ et $k\in[\![2,n]\!]$. Alors k est diviseur de $n!$ et de k donc k divise $n!+k$.
Comme k n'est ni 1, ni $n!+k$, on en déduit que $n!+k$ n'est pas premier.
On en déduit qu'il existe des séquences de nombres entiers aussi grandes que souhaitées telles qu'aucun d'entre eux ne soit premier.

Solution 16 –

1. D'après la formule de factorisation de $x^n - y^n$, on a

$$a^p - 1 = (a-1)\left(\sum_{k=0}^{p-1} a^k\right).$$

Si $a \neq 2$, alors $a - 1 \geqslant 2$ et $\left(\sum_{k=0}^{p-1} a^k\right) \geqslant 2$ (car $p \geqslant 2$).

Donc $a^p - 1$ n'est pas premier, ce qui est absurde. D'où $a = 2$.

2. (a) On a

$$2^{pq} - 1 = (2^p)^q - 1^q = (2^p - 1)\sum_{k=0}^{q-1} 2^{pk} 1^{q-1-k}$$

Donc $2^p - 1$ divise $2^{pq} - 1$.

(b) On procède par contraposée.

Soit $n \in \mathbb{N}$ non-premier. Si $n = 0$, alors $2^n - 1 = 0$, qui n'est pas premier.

Si $n = 1$, alors $2^n - 1 = 1$, qui n'est pas premier.

Si $n \geqslant 4$, alors il existe p et q entiers supérieurs ou égaux à 2 tels que $n = pq$. Alors, d'après la question 1, $2^n - 1$ est divisible par $2^p - 1$, qui n'est ni égal à 1, ni égal à $2^n - 1$. Donc $2^n - 1$ n'est pas premier.

Par contraposée, si $2^n - 1$ est premier, alors n est premier.

(c) On propose un programme python (certes peu efficace) pour tester la primalité des premiers nombres $2^n - 1$.

```
from math import sqrt
def est_premier(n:int)->bool:
    """ Détermine si un entier naturel est premier"""
    if n==0 or n==1:
        return False
    for i in range(2,1+int(sqrt(n))):
        if n%i == 0:
            return False
    return True

def mersenne(borne:int)->int:
    """    Cherche un nombre non-premier de la forme
       ↪ 2**p-1 avec p premier    """
    for p in range(borne):
        if est_premier(p):
            M = 2**p - 1
            if not est_premier(M):
                return p
    return 0
```

On en déduit que si $n = 11$, alors $2^n - 1 = 2047$, qui n'est pas premier car $2047 = 23 \times 89$.

La réciproque est donc fausse.

3. On pose $N = 2^{p-1}M$. Comme M est premier, $2^{p-1}M$ est une décomposition en facteurs premiers de N. On peut alors lister les diviseurs de N :

$$1, 2, 2^2, \ldots, 2^{p-1}.$$

$$M, 2M, 2^2M, \ldots, 2^{p-1}M.$$

Reste à calculer la somme :

$$\begin{aligned}\sum_{d\in\mathbb{N}, d|n} d &= \sum_{i=0}^{p-1} 2^i + \sum_{i=0}^{p-1} M2^i \\ &= (1+M)\sum_{i=0}^{p-1} 2^i \\ &= (1+M)\frac{2^p - 1}{2-1} \\ &= 2^p(2^p - 1) \\ &= 2.2^{p-1}M = 2N\end{aligned}$$

Donc N est parfait.

Pour s'instruire sur les nombres parfaits :
The Oldest Unsolved Problem in Math - - Veritasium

Solution 17 –

1. *Analyse.* Soit $(x, y) \in \mathbb{N}^2$ vérifiant le système. En posant $x' = \frac{x}{3}$ et $y' = \frac{y}{3}$, on a :

$$\begin{cases} x' \wedge y' &= 1 \\ x' + y' &= 7 \end{cases}$$

Puisque $x' + y' = 7$, on a

$$(x', y') \in \{(0,7), (1,6), (2,5), (3,4), (4,3), (5,2), (6,1), (7,0)\},$$

$$(x, y) \in \{(0,21), (3,18), (6,15), (9,12), (12,9), (15,6), (18,3), (21,0)\}.$$

Synthèse.

(a) On a $0 \wedge 21 = 21$ donc $(0,21)$ n'est pas solution.
(b) On a $3 \wedge 18 = 3$, donc $(3,18)$ est solution.
(c) On a $6 \wedge 15 = 3$, donc $(6,15)$ est solution.
(d) On a $9 \wedge 12 = 3$, donc $(9,12)$ est solution.
(e) Les autres cas s'obtiennent à partir de ceux déjà traités, par symétrie du problème.

Finalement, l'ensemble des solutions est
$\{(3,18),(6,15),(9,12),(12,9),(15,6),(18,3)\}$.

2. Soit $(x,y) \in \mathbb{N}^2$.

$$\begin{cases} x \wedge y &= 6 \\ x \vee y &= 72 \end{cases} \iff \exists (x',y') \in \mathbb{Z}^2, \begin{cases} x &= 6x' \\ y &= 6y' \\ x' \wedge y' &= 1 \\ x' \vee y' &= 12 \end{cases}.$$

Intéressons-nous au problème

$$(S) \quad \begin{cases} x' \wedge y' &= 1 \\ x' \vee y' &= 12 \end{cases},$$

d'inconnue $(x',y') \in \mathbb{N}^2$.
Analyse. Soit $(x',y') \in \mathbb{N}^2$ vérifiant le système (S). On a :

$$\begin{cases} x' \wedge y' &= 1 \\ x'y' &= 12 \end{cases}$$

Puisque $x'y' = 12$, on en déduit que
$(x',y') \in \{(1,12),(2,6),(3,4),(4,3),(6,2),(12,1)\}$.
Synthèse.

(a) $1 \wedge 12 = 1$, donc $(1,12)$ est une solution.
(b) $2 \wedge 6 = 2$, donc $(2,6)$ n'est pas une solution.
(c) $3 \wedge 4 = 1$, donc $(3,4)$ est une solution.
(d) Les autres cas s'obtiennent à partir de ceux déjà traités, par symétrie du problème.

Finalement, les solutions de (S) sont $(1,12)$, $(3,4)$, $(4,3)$ et $(12,1)$. On en déduit que l'ensemble des solutions du problème initial est :

$$\{(6,72),(12,36),(18,24),(24,18),(36,12),(72,6)\}.$$

Solution 18 –

1. $\mathrm{Div}\left(p^\alpha\right) \cap \mathbb{N} = \{1,p,p^2,\dots,p^\alpha\}$ donc $\sigma\left(p^\alpha\right) = \dfrac{p^{\alpha+1}-1}{p-1}$.

2. Soit $d \in \mathrm{Div}(ab) \cap \mathbb{N}$. Posons $d_1 = \mathrm{pgcd}(d,a)$ et $d_2 = \mathrm{pgcd}(d,b)$.
On a $d_1 \in \mathrm{Div}(a) \cap \mathbb{N}$ et $d_2 \in \mathrm{Div}(b) \cap \mathbb{N}$. Puisque $a \wedge b = 1$ on a $d_1 \wedge d_2 = 1$. Or $d_1 \mid d$ et $d_2 \mid d$ donc $d_1 d_2 \mid d$. $d_1 = du_1 + av_1$ et $d_2 = du_2 + bv_2$ donc $d_1 d_2 = dk + abv_1 v_2$ d'où $d \mid d_1 d_2$.
Finalement $d = d_1 d_2$. Supposons $d = \delta_1 \delta_2$ avec $\delta_1 \in \mathrm{Div}(a) \cap \mathbb{N}$ et $\delta_2 \in \mathrm{Div}(b) \cap \mathbb{N}$. On a $d_1 \mid \delta_1 \delta_2$ et $d_1 \wedge \delta_2 = 1$ donc $d_1 \mid \delta_1$ et de même $\delta_1 \mid d_1$ puis $d_1 = \delta_1$. De même $d_2 = \delta_2$.

3. $\sigma(ab) = \displaystyle\sum_{d \mid ab} d = \sum_{d_1 \mid a} \sum_{d_2 \mid b} d_1 d_2 = \left(\sum_{d_1 \mid a} d_1\right)\left(\sum_{d_2 \mid b} d_b\right) = \sigma(a)\sigma(b)$.

4. Si $n = p_1^{\alpha_1} \dots p_N^{\alpha_N}$ alors $\sigma(n) = \displaystyle\prod_{i=1}^{N} \frac{p_i^{\alpha_{i+1}-1}}{p_i - 1}$.

Solution 19 –

1.

$$\begin{aligned} 2^a - 1 &= 2^{bq+r} - 1 \\ &= 2^r \times (2^{bq} - 1) + 2^r - 1 \\ &= 2^r \times (2^b - 1)\left(\sum_{k=0}^{q-1} 2^{bk}\right) + 2^r - 1 \end{aligned}$$

De plus, $0 \leqslant 2^r - 1 < 2^b - 1$, donc par unicité du reste et du quotient de la division euclidienne, la division euclidienne de $2^a - 1$ par $2^b - 1$ a pour quotient $2^r \dfrac{2^{bq}-1}{2^b-1}$ et pour reste $2^r - 1$.

2. D'après un résultat du cours,

$$\left(2^a - 1\right) \wedge \left(2^b - 1\right) = \left(2^b - 1\right) \wedge \left(2^r - 1\right).$$

Ainsi, en notant $r_0 = b$, $r_1 = r$, puis $r_2, r_3, \dots, r_{\ell+1}$ où pour tout i, r_i est le reste de la division euclidienne de r_{i-2} par r_{i-1}. D'après l'algorithme d'Euclide, il existe ℓ tel que $r_{\ell+1} = 0$ et $r_\ell = a \wedge b$
D'après la question 1 et le résultat du cours, pour tout $i \in [\![0, \ell-1]\!]$,

$$\left(2^{r_i} - 1\right) \wedge \left(2^{r_{i+1}} - 1\right) = 2^{r_{i+2}} - 1.$$

D'après l'algorithme d'Euclide, le dernier reste non-nul est $2^{a \wedge b} - 1$ (le suivant est $2^0 - 1$, qui est bien nul), donc

$$\left(2^a - 1\right) \wedge \left(2^b - 1\right) = 2^{a \wedge b} - 1.$$

Solution 20 –

1. $v_2(1000!) = 500 + v_2(500!)$ car $1000! = 2^{500} \times 500! \times k$ avec k produit de nombres impairs.
$$v_2(1000!) = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994$$
2. 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
$$k = \left\lfloor \frac{\ln n}{\ln p} \right\rfloor .$$

Solution 21 – Par hypothèse, on peut écrire $n = p_1 p_2 \dots p_r$ avec $p_1, \dots, p_r$ nombres premiers deux à deux distincts. Soit $a \in \mathbb{Z}$. Considérons $i \in \{1, \dots, r\}$. Si p_i ne divise pas a, le petit théorème de Fermat assure $a^{p_i - 1} \equiv 1 \,[p_i]$. Puisque $p_i - 1$ divise $n - 1$, on a encore $a^{n-1} \equiv 1 \,[p_i]$ et donc $a^n \equiv a \,[p_i]$ Si p_i divise a alors p_i divise aussi a^n et donc $a^n \equiv 0 \equiv a \,[p_i]$. Enfin, chaque p_i divisant $a^n - a$ et les p_i étant deux à deux premiers entre eux, $n = p_1 \dots p_r$ divise $a^n - a$ et finalement $a^n \equiv a[n]$. La réciproque de ce résultat est vraie. Ce résultat montre que le petit théorème de Fermat ne caractérise pas les nombres premiers. Les nombres non premiers satisfaisant le petit théorème de Fermat, sont les nombres de Carmichael. Le plus petit d'entre eux est 561 , le suivant 1105 .

Quelques vidéos pour se cultiver:
Un peu d'histoire sur les conjectures des nombres premiers :
Les nombres premiers - - Science Etonnante

Un détour par la cryptographie :
L'Algorithme qui Sécurise Internet (entre autres...) - - Science Etonnante

♣ Du trèfle à brouter... ♠ Qui s'y frotte s'y pique !

♥ À connaître par cœur. ♦ Calculatoire, risque de rester sur le carreau !