$\boxed{\text{TD 9}}$ - Arithmétique

$\boxed{\text{Ex 1}}$: a)

$$\begin{array}{r|l} 2867 & 6 \\ \cline{2-2} \underline{24} & 477 \\ 467 & \\ \underline{42} & \\ 47 & \\ \underline{42} & \\ 5 & \end{array}$$

donc $2867 = 6 \times 477 + 5$

b)

$$\begin{array}{r|l} 7813 & -12 \\ \cline{2-2} \underline{72} & -651 \\ 613 & \\ \underline{60} & \\ 13 & \\ \underline{12} & \\ 1 & \end{array}$$

$7813 = -12 \times (-651) + 1$

c)

$$\begin{array}{r|l} -959 & 6 \\ \cline{2-2} \underline{-6} & -150 - 10 \\ -359 & = -160 \\ \underline{-30} & \\ -59 & \\ \underline{-60} & \\ 1 & \end{array}$$

$-959 = 6 \times (-160) + 1$

d)

$$\begin{array}{r|l} -1733 & -5 \\ \cline{2-2} \underline{-15} & 347 \\ -233 & \\ \underline{-20} & \\ -33 & \\ \underline{-35} & \\ 2 & \end{array}$$

$-1733 = -5 \times 347 + 2$

$\boxed{\text{Ex 2}}$ $(a,b) \in \mathbb{N} \times \mathbb{N}^*$.

1. Si $x \in \mathbb{R}$ et $k \in \mathbb{N}^*$, $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \dots + x + 1)$

Par conséquent, $b | a \Rightarrow \exists k \in \mathbb{N}$ tel que $a = bk$.

$\underline{k=0} \Rightarrow a = 0$, donc $2^a - 1 = 0$ et $2^b - 1 \mid 2^a - 1$.

$\underline{k>0} \Rightarrow 2^a - 1 = 2^{kb} - 1$

$$= (2^b)^k - 1 = (2^b - 1)(2^{b(k-1)} + \dots + 1)$$

donc $2^b - 1 \mid 2^a - 1$.

2. Soit r le reste dans la division euclidienne de a par b :

$\exists k \in \mathbb{N}$ tq $a = bk + r$, et $0 \leq r < b$.

Alors $2^a - 1 = 2^{bk+r} - 1 = 2^r \underbrace{(2^{bk} - 1)}_{\text{multiple de } 2^b - 1 \text{, donc}} + 2^r - 1$

$$= q(2^b - 1) + 2^r - 1$$

pour un certain $q \in \mathbb{N}$. De plus, $0 \leq r < b \Rightarrow 0 \leq 2^r - 1 < 2^b - 1$

donc $2^r - 1$ est le reste dans la division euclidienne de $2^a - 1$ par $2^b - 1$

$\boxed{\text{Ex } 3}$: $7a - 4b^3 = 1 \Rightarrow -4b^3 \equiv 1\ [7]$

$\Rightarrow -8b^3 \equiv 2\ [7]$

$\Rightarrow b^3 \equiv -2\ [7]$.

Or, on connaît tous les restes possibles des cubes modulo 7 :

$b \equiv 0\ [7] \Rightarrow b^3 \equiv 0\ [7]$

$b \equiv 1\ [7] \Rightarrow b^3 \equiv 1\ [7]$

2	$\Rightarrow$	$8 \equiv 1\ [7]$
3	$\Rightarrow$	$27 \equiv 3\ [7]$
$4 \equiv -3$	$\Rightarrow$	$\equiv -3\ [7]$
$5 \equiv -2$	$\Rightarrow$	$\equiv -1\ [7]$
$6 \equiv -1$	$\Rightarrow$	$\equiv -1\ [7]$

donc $b^3 \equiv -2\ [7]$ est impossible, et a fortiori il n'existe pas (a, b) dans $\mathbb{Z}^2$ tq $7a - 4b^3 = 1$.

$\boxed{\text{Ex } 4}$: 1. (a) $7^2 = 49 = 4 \times 12 + 1 \equiv 1\ [12]$, $k_0 = 2$ convient

(b) $6^2 = 36 = 3 \times 12 \equiv 0\ [12]$, $k_1 = 2$ convient.

(c) $3^2 = 9$, $3^3 = 27 = 12 \times 2 + 3 \equiv 3\ [12]$, $(k_2, k_3) = (1, 3)$ convient.

(d) $7^{30} = (7^2)^{15} \equiv 1^{15} \equiv 1\ [12]$

$6^{13} = 6^2 \cdot 6^{11} \equiv 0\ [12]$

$3^{17} = 3^3 \cdot 3^{14} \equiv 3 \cdot 3^{14} \equiv 3^{15} \equiv 3^{13} \equiv \dots \equiv 3^1 \equiv 3\ [12]$.

$31^{77} = (2 \times 12 + 7)^{77} \equiv 7^{77} \equiv 7^{38 \times 2 + 1} \equiv 7\ [12]$

$19^5 + 30^{144} + 15^{10} \equiv 7^5 + 6^{144} + 3^{10}\ [12]$

$\equiv 7^{2 \times 2 + 1} + 6^2\, 6^{142} + 3^{2+2+2+2+2}\ [12]$

$\equiv 7 + 0 + 3^2\ [12]$

$\equiv 4\ [12]$.

2. 11 est premier, et donc, d'après le petit théorème de Fermat,

$2^{11} \equiv 2\ [11]$ et $3^{11} \equiv 3\ [11]$.

$\Rightarrow (2^{11})^{11} = 2^{121} \equiv 2^{11} \equiv 2\ [11]$ et $3^{121} \equiv 3\ [11]$

$\Rightarrow 2^{123} + 3^{121} \equiv 4 \times 2^{121} + 3^{121}$

$\equiv 4 \times 2 + 3\ [11]$

$\equiv 0\ [11]$

donc $11 \mid 2^{123} + 3^{121}$.

3. $122 = 117+5 = 13\times 9 + 5$, donc $122 \equiv 5\ [9]$

$5^2 = 25 \equiv 7\ [9]$

$5^3 \equiv 35 \equiv -1\ [9]$, donc $5^6 \equiv 1\ [9]$

$137 = 6\times 22 + 5$, donc $122^{137} \equiv 5^{6\times 22+5}\ [9]$

$\equiv 5^5\ [9]$

$\equiv 5^2 \cdot 5^3 \equiv -7 \equiv 2\ [9]$

$\boxed{\text{Ex 5}}$: $3^2 = 9 \equiv -1\ [10]$, donc $3^4 \equiv 1\ [10]$.

Par conséquent, $3^{1111} = 3^{4\times 277+3} \equiv 3^3\ [10]$

$\equiv 7\ [10]$

et le dernier chiffre de 3^{1111} dans son écriture décimale est 7.

$\boxed{\text{Ex 6}}$: 1. $230 = 126\times 1 + 104$

$126 = 104\times 1 + 22$

$104 = 22\times 4 + 16$

$22 = 16\times 1 + 6$

$16 = 6\times 2 + 4$

$6 = 4\times 1 + 2$

$4 = 2\times 2 + 0$

donc pgcd $(230, 126)$

$=$ pgcd $(126, 104)$

$=$ pgcd $(104, 22)$

$=$

$\vdots$

$=$ pgcd $(4, 2)$

$= 2$.

2. Soit $(a,b,c) \in \mathbb{Z}^3$, $n \in \mathbb{Z}$

On sait que $(n|a$ et $n|b) \Leftrightarrow (n|\text{pgcd}(a,b))$ (grâce au th. de Bézout)

Ainsi, $(n|a$ et $n|b$ et $n|c) \Leftrightarrow (n|\text{pgcd}(a,b)$ et $n|c)$

et donc $(n|\text{pgcd}(a,b)$ et $n|c) \Leftrightarrow (n|a$ et $n|b$ et $n|c)$

$\Leftrightarrow (n|a$ et $n|\text{pgcd}(b,c))$

et donc, par définition du pgcd,

$\text{pgcd}(\text{pgcd}(a,b), c) = \text{pgcd}(a, \text{pgcd}(b,c))$.

3. a) pgcd $(720, 390)$ = pgcd $(390, 330)$

= pgcd $(330, 60)$

= 30

pgcd $(390, 720, 450)$

= pgcd $(30, 450)$

= 30.

b) pgcd $(180, 606)$ = pgcd $(180, 66)$

= pgcd $(66, 48)$ = pgcd $(48, 18)$ = pgcd $(18, 12)$ = 6 donc $\text{pgcd}(180, 606, 750) = \text{pgcd}(6, 750) = 6$.

$\boxed{\text{Ex } 7}$: a) $\text{pgcd}(m,n) = 18$ et $m+n = 360$

$$\iff \begin{cases} m = 18a \\ n = 18b \\ \text{pgcd}(a,b) = 1 \end{cases} \quad \text{et} \quad 18(a+b) = 360$$

$$\iff \begin{cases} m = 18a \\ n = 18b \\ \text{pgcd}(a,b) = 1 \end{cases} \quad \text{et} \quad a+b = 20$$

On cherche toutes les solutions premières entre elles de $a+b=20$:

$(19,1)$ $(1,19)$
$(17,3)$ $(3,17)$
$(13,7)$ $(7,13)$
$(11,9)$ $(9,11)$

donc $\{(m,n) \in \mathbb{N}^2 \,/\, \text{pgcd}(m,n) = 18 \text{ et } m+n = 360\}$

$= \{(18\times 19, 18), (18\times 17, 3\times 18), (13\times 18, 7\times 18), (11\times 18, 9\times 18),$
$(18, 18\times 19), (3\times 18, 17\times 18), (7\times 18, 13\times 18), (9\times 18, 11\times 18)\}$

b) $\text{pgcd}(m,n) = 18$ et $mn = 6480$ $(*)$

$$\iff \begin{cases} m = 18a \\ n = 18b \\ \text{pgcd}(a,b) = 1 \end{cases} \quad \text{et} \quad 18^2 ab = 6480 = 18 \times 360 = 18^2 \times 20$$

on cherche les sol. de $ab = 20$, $\text{pgcd}(a,b) = 1$:

$(1,20)$ $(20,1)$
$(4,5)$ $(5,4)$

donc les solutions de $(*)$ sont $\{(18, 360), (360, 18), (72, 90), (90, 72$

$\boxed{\text{Ex } 8}$: $(a,b) \in \mathbb{Z}^2$.

1. On suppose que $\text{pgcd}(a,b) = 1$. Soit $(p,q) \in \mathbb{Z}^2$.

$\Leftarrow$: ~~on suppose qu'il $\exists\, k \in \mathbb{Z}$ tq p Soit $(p,q) \in \mathbb{Z}^2$~~. On suppose qu'il existe $k \in \mathbb{Z}$ tq $p = bk$ et $q = ak$, alors $ap = abk = bq$.

$\Rightarrow$: on suppose que $ap = bq$. Comme $\text{pgcd}(a,b) = 1$, le th. de Gauss implique qu'il existe $k \in \mathbb{Z}$ tq $q = ka$. Par conséquent,

$$ap = qb = akb \Rightarrow \begin{cases} p = kb & \text{si } a \neq 0 \\ q = 0 \text{ et } b = \pm 1 & \text{si } a = 0 \\ \text{et donc } p = \pm bp \\ q = \pm bq \end{cases}$$

d'où l'équivalence : $(ap = bq) \Leftrightarrow (\exists k \in \mathbb{Z} \text{ tq } p = bk \text{ et } q = ak)$

2. On suppose que $(ap = bq) \Leftrightarrow (\exists k \in \mathbb{Z} \text{ tq } p = bk \text{ et } q = ak)$.

Soit $d = \text{pgcd}(a,b) \Rightarrow \exists (p,q)$ tq $\begin{cases} a = dq \\ b = dp \end{cases}$

et donc $ap = dpq = bq$

$\Rightarrow \exists k \in \mathbb{Z}$ tq $p = bk$ et $q = ak$

$\Rightarrow \begin{cases} p = p\,dk \\ q = q\,dk \end{cases} \Rightarrow dk = 1 \Rightarrow d = 1$

donc $\text{pgcd}(a,b) = 1$.

$\boxed{\text{Ex 9}}$: a) $18a + 5b = 11$ $(*)$

$\text{pgcd}(18,5) = 1$:

$$\begin{aligned}
18 &= 5 \times 3 + 3 & &= 1 \times 18 + 0 \times 5 \\
5 &= 3 \times 1 + 2 & &= 0 \times 18 + 1 \times 5 \\
3 &= 2 \times 1 + 1 = 18 - 5 \times 3 & &= 1 \times 18 - 3 \times 5 \\
2 &= 1 \times 2 + 0 = 5 - 3 \times 1 & &= -1 \times 18 + 4 \times 5 \\
1 &= = 3 - 2 \times 1 & &= 2 \times 18 - 7 \times 5
\end{aligned}$$

$\Rightarrow$

donc $18 \times 2 - 5 \times 7 = 1$

$\Rightarrow (a,b) = (22, -77)$ est une solution de $(*)$

$18a + 5b = 11 \Leftrightarrow 18a + 5b = 18 \times 22 - 5 \times 77$

$\Leftrightarrow 18(a - 22) = 5(-b - 77)$

$\Leftrightarrow \exists k \in \mathbb{Z}$ tq $\begin{cases} a - 22 = 5k \\ -b - 77 = 18k \end{cases}$

donc $\{(a,b) \in \mathbb{Z}^2 / 18a + 5b = 11\} = \{(22 + 5k, -77 - 18k),\ k \in \mathbb{Z}\}$.

b) $39a - 12b = 121$ $\qquad \text{pgcd}(39, 12) = 3$

et $3 \nmid 121$, donc il n'y a pas de solution.

c) ~~[illegible]~~ $14a - 21b = 49$ —

$\operatorname{pgcd}(14,21) = 7$, donc $14a - 21b = 49$

$\iff 2a - 3b = 7 \quad (*)$

On trouve facilement une relation de Bézout :

$$2\times 2 - 3\times 1 = 1$$

et donc $(a,b) = (14,+7)$ est une solution de $(*)$.

$2a - 3b = 7 = 2\times 14 - 3\times 7 \iff 2(a-14) = 3(b-7)$

$\iff \exists k \in \mathbb{Z}$ tq $\begin{cases} a-14 = 3k \\ b-7 = 2k \end{cases}$

donc $\{(a,b)\in\mathbb{Z}^2,\ 14a - 21b = 49\} = \{(3k+14,\ 2k+7),\ k\in\mathbb{Z}\}$.

$\boxed{\text{Ex10}}$: a) $\begin{cases} n \equiv 1\ [20] \\ n \equiv 3\ [7] \end{cases}$ $\operatorname{pgcd}(20,7) = 1$.

On commence par chercher une relation de Bézout :

$$-20 + 3\times 7 = 1$$

on pose donc $n_0 = (-20)\times 3 + (3\times 7)\times 1 = -39$

$n_0 \equiv 3\times 7\times 1\ [20]$ $\qquad$ $n_0 \equiv (-20)\times 3\ [7]$

$\equiv (-20+3\times 7)\ [20]$ $\qquad$ $\equiv (-20+3\times 7)\times 3\ [7]$

$\equiv 1\ [20]$ $\qquad$ $\equiv 3\ [7]$

donc n_0 est une solution particulière.

Maintenant, $n\in\mathbb{Z}$ vérifie $\begin{cases} n\equiv 1\ [20] \\ n\equiv 3\ [7] \end{cases} \iff \begin{cases} n\equiv n_0\ [20] \\ n\equiv n_0\ [7] \end{cases}$

$\iff$ 20 et 7 divisent $n - n_0$

$\iff$ 140 divise $n - n_0$ (car $\operatorname{pgcd}(20,7) = 1$), donc $\operatorname{ppcm}(20,7) = 140$

$\iff \exists k\in\mathbb{Z}$ tq $n = 140k + n_0$.

b) $\begin{cases} n\equiv 13\ [15] \\ n\equiv 6\ [10] \end{cases}$ $\operatorname{pgcd}(15,10) = 5$

Soit $n\in\mathbb{Z}$. $\begin{cases} n\equiv 13\ [15] \\ n\equiv 6\ [10] \end{cases} \Rightarrow \begin{cases} n\equiv 3\ [5] \\ n\equiv 1\ [5] \end{cases}$, c'est exclu.

Il n'y a donc pas de solution.

c) $\begin{cases} n \equiv 11 \,[15] \\ n \equiv 6 \,[10] \end{cases}$ cette fois, $11 \equiv 6 \,[5]$, donc on cherche une solution particulière :

Si n est solution, alors $n-1 \equiv 0 \,[5]$, donc $\exists m \in \mathbb{Z}$ tq $n-1 = 5m$. De plus,

$$\begin{cases} n-1 \equiv 10 \,[15] \\ n-1 \equiv 5 \,[10] \end{cases} \Leftrightarrow \begin{cases} m \equiv 2 \,[3] \\ m \equiv 1 \,[2] \end{cases}$$

On cherche une solution particulière, avec la relation de Bézout :

$$3 - 2 = 1$$

Soit $m_0 = 1 \times 3 - 2 \times 2 = -1$, m_0 est une solution particulière, et donc $\begin{cases} m \equiv 2 \,[3] \\ m \equiv 1 \,[2] \end{cases} \Leftrightarrow \exists k \in \mathbb{Z} \,/\, m = m_0 + k \cdot 2 \cdot 3$
$= m_0 + 6k.$

et finalement, $n \in \mathbb{Z}$ vérifie $\begin{cases} n \equiv 11 \,[15] \\ n \equiv 6 \,[10] \end{cases}$

$$\Leftrightarrow \exists k \in \mathbb{Z} \text{ tq } n = 1 + 5 \times (m_0 + 6k) = -4 + 30k.$$

d) $\begin{cases} n \equiv 3 \,[224] \\ n \equiv 17 \,[119] \end{cases}$

$$224 = 119 \times 1 + 105$$
$$119 = 105 \times 1 + 14$$
$$105 = 14 \times 7 + 7$$
$$14 = 7 \times 2 + 0$$

$\Rightarrow \operatorname{pgcd}(224, 119) = 7$. Si n est solution, alors $n - 3 \equiv 0 \,[7]$, donc $\exists m \in \mathbb{Z}$ tq $n - 3 = 7m$, et

$$\begin{cases} n-3 \equiv 0 \,[224] \\ n-3 \equiv 14 \,[119] \end{cases} \Leftrightarrow \begin{cases} m \equiv 0 \,[32] \\ m \equiv 2 \,[17] \end{cases}$$

On cherche une relation de Bézout entre 32 et 17 :

$$32 = 17 \times 1 + 15 \qquad = 1 \times 32 + 0 \times 17$$
$$17 = 15 \times 1 + 2 \qquad = 0 \times 32 + 1 \times 17$$
$$15 = 2 \times 7 + 1 \quad = 32 - 17 \times 1 = 1 \times 32 - 1 \times 17$$
$$2 \quad = 17 - 15 \times 1 = -1 \times 32 + 2 \times 17$$
$$1 \quad = 15 - 2 \times 7 = 8 \times 32 - 15 \times 17$$

donc $8 \times 32 - 15 \times 17 = 1$

on pose $m_0 = 2 \times 8 \times 32 - 0 = 512$, c'est une solution particulière, et donc $\begin{cases} n \equiv 3 \,[224] \\ n \equiv 17 \,[119] \end{cases} \Leftrightarrow \exists k \in \mathbb{Z}$ tq $n = 3 + 7(512 + 32 \times 17 \times k)$
$= 3587 + 3808k$

Ex 11 : 1. $(a,b) \in \mathbb{Z}^2$

$\Rightarrow$ Supposons que $\operatorname{pgcd}(a,b) = 1$. Soit alors $d \in \mathbb{N}^*$ un diviseur commun de ab et $a+b$.

$$\begin{cases} d \mid a+b \\ d \mid ab \end{cases} \Rightarrow \begin{cases} d \mid a(a+b) \text{ et } d \mid b(a+b) \\ d \mid ab \end{cases} \Rightarrow \begin{cases} d \mid a^2+ab \text{ et } d \mid b^2+ab \\ d \mid ab \end{cases}$$

$$\Rightarrow d \mid a^2 \text{ et } d \mid b^2$$

$$\Rightarrow d \mid \text{pgcd}(a^2, b^2) = (\text{pgcd}(a,b))^2 = 1$$

$$\Rightarrow d = 1$$

donc $\text{pgcd}(ab, a+b) = 1$.

$\underline{\Leftarrow}$. Supposons maintenant que $\text{pgcd}(ab, a+b) = 1$. Alors, comme

$\text{pgcd}(a,b) \mid a$ et b,

$\text{pgcd}(a,b) \mid ab$ et $a+b$ $\Rightarrow \text{pgcd}(a,b) \mid \text{pgcd}(ab, a+b)$

$\Rightarrow \text{pgcd}(a,b) = 1$.

On a donc montré que $\text{pgcd}(a,b) = 1 \Leftrightarrow \text{pgcd}(ab, a+b) = 1$.

2. $a = b = 2$ donne : $\text{pgcd}(a,b) = 2$

$\text{pgcd}(a+b, ab) = 4$.

$\boxed{\text{Ex } 12}$ Soit $n \in \mathbb{N}$.

$$\frac{n+2}{n+9} \text{ est réductible} \Leftrightarrow \exists k \in \mathbb{N}\setminus\{0,1\} \text{ tq } \begin{cases} k \mid n+2 \\ k \mid n+9 \end{cases}$$

$$\Leftrightarrow \exists k \in \mathbb{N}\setminus\{0,1\} \text{ tq } \begin{cases} k \mid n+2 \\ k \mid 7 \end{cases}$$

$$\Leftrightarrow 7 \mid n+2$$

donc $\frac{n+2}{n+9}$ est irréductible ssi $n \not\equiv 5\ [7]$.

$\boxed{\text{Ex } 13}$: 1. Soit $n > 1$ un entier, et $k \mid n$, k impair.

Il existe donc $m \in \mathbb{N}$ tq $n = km$, et alors

$$2^n + 1 = 2^{km} - (-1)^k = (2^m)^k - (-1)^k$$

$$= (2^m + 1)\left((2^m)^{k-1} - (2^m)^{k-2} + \ldots \mp 2^m + 1\right)$$

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

donc $2^m + 1$ divise $2^n + 1$.

Par conséquent, si $2^n + 1$ est premier, alors $n = km$ avec k impair

$\Rightarrow k = 1$ et $m = n$

n n'admet aucun diviseur impair différent de 1, c'est donc une puissance de 2.

2. $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$

(a) $F_0 = 2^1 + 1 = 3$ $\qquad$ $F_3 = 2^8 + 1 = 257$

$F_1 = 2^2 + 1 = 5$ $\qquad$ $F_4 = 2^{16} + 1 = 65\,537$

$F_2 = 2^4 + 1 = 17$

(b) $F_1 = F_0 + 2$. Montrons par récurrence que $\forall n \in \mathbb{N}$, $F_{n+1} = \left(\prod_{k=0}^{n} F_k\right) + 2$

C'est vrai pour $n = 0$. Supposons la propriété vraie pour $n \in \mathbb{N}$.

Alors $(F_{n+1})^2 = \left(\prod_{k=0}^{n+1} F_k\right) + 2F_{n+1}$

Or, $(F_{n+1})^2 = \left(2^{2^{n+1}}\right)^2 + 2 \cdot 2^{2^{n+1}} + 1$

$= 2^{2^{n+2}} + 1 + 2 \cdot 2^{2^{n+1}}$

$= F_{n+2} + 2(F_{n+1} - 1)$

et donc $F_{n+2} + \cancel{2F_{n+1}} - 2 = \prod_{k=0}^{n+1} F_k + \cancel{2F_{n+1}}$

$\Rightarrow F_{n+2} = \prod_{k=0}^{n+1} F_k + 2.$

La propriété est donc vraie $\forall n \in \mathbb{N}$.

(c) Soient $n, m \in \mathbb{N}$, $n \neq m$. On peut supposer, sans perte de généralité, que $n < m$. Alors $F_m = \prod_{k=0}^{m-1} F_k + 2$

et donc $F_m - \left(\prod_{\substack{k \in [\![0;m-1]\!] \\ k \neq n}} F_k\right) F_n = 2$

d'où $\mathrm{pgcd}(F_m, F_n) \mid 2$

Or, F_m et F_n sont impairs ; d'où finalement F_m et F_n sont premiers entre eux.

3. Si on note, pour $n \in \mathbb{N}$, p_n le plus petit premier divisant F_n, on déduit de la question (c) que $\forall n \neq m$, $p_n \neq p_m$, et donc $\{p_n, n \in \mathbb{N}\}$ est infini, et a fortiori l'ensemble des nombres premiers est infini.

$\boxed{\text{Ex 14}}$: 1. $12 = 2^2 \times 3$

2. {diviseurs de 12} = {1, 2, 3, 4, 6, 12}.

$\boxed{\text{Ex 15}}$: 1. Soit $N \in \mathbb{N}^*$. On note $N = \prod_{k=0}^{n} p_k^{\alpha_k}$ sa décomposition en nombres premiers, $\alpha_k \in \mathbb{N}$ $\forall k \in [\![0;n]\!]$, $p_k \in \mathcal{P}$

Les diviseurs de N sont alors les entiers de forme

$$\prod_{k=0}^{n} p_k^{\beta_k} \quad , \text{ avec } \beta_k \in [\![0;\alpha_k]\!] \ \forall k \in [\![0;n]\!].$$

Par conséquent, la fonction

$$\varphi : \prod_{k=0}^{n} [\![0;\alpha_k]\!] \longrightarrow \{ d \in \mathbb{N},\ d \mid N \}$$
$$(\beta_0, \dots \beta_n) \longmapsto \prod_{k=0}^{n} p_k^{\beta_k}$$

est une bijection, et donc

$$\sigma_0(N) = \mathrm{Card}\{ d \in \mathbb{N},\ d\mid N\} = \prod_{k=0}^{n} \mathrm{Card}([\![0;\alpha_k]\!])$$
$$= \prod_{k=0}^{n} (\alpha_k + 1)$$

Par ailleurs,

$$\sigma_1(N) = \sum_{\substack{0 \le \beta_0 \le \alpha_0 \\ \vdots \\ 0 \le \beta_n \le \alpha_n}} \prod_{k=0}^{n} p_k^{\beta_k} = \sum_{\beta_n = 0}^{\alpha_n} \left(p_n^{\beta_n} \left(\sum_{\substack{0 \le \beta_0 \le \alpha_0 \\ \vdots \\ 0 \le \beta_{n-1} \le \alpha_{n-1}}} \prod_{k=0}^{n-1} p_k^{\beta_k} \right)\right)$$

$$= \left(\sum_{\beta_n = 0}^{\alpha_n} p_n^{\beta_n} \right) \left(\sum_{\substack{0 \le \beta_0 \le \alpha_0 \\ \vdots \\ 0 \le \beta_{n-1} \le \alpha_{n-1}}} \prod_{k=0}^{n-1} p_k^{\beta_k} \right)$$

$$\overset{\text{récurrence}}{(\dots)} = \prod_{k=0}^{n} \left(\sum_{\beta_k = 0}^{\alpha_k} p_k^{\beta_k} \right) = \prod_{k=0}^{n} \left(\frac{1 - p_k^{\alpha_k + 1}}{1 - p_k} \right).$$

2. $N \in \mathbb{N}$, $\begin{cases} \sigma_0(N) = 6 = 2 \times 3 \\ \sigma_1(N) = 28 = 2^2 \times 7 \end{cases} \Rightarrow$ N s'écrit $N = p_0^1 p_1^2$ avec p_0, p_1 des nombres premiers

et $(1+p_0)(1+p_1+p_1^2) = 28$

Si $p \in \mathcal{P}$, alors $1 + p + p^2 \geqslant 1 + 2 + 2^2 = 7$, donc nécessairement, $p_1 = 2$, et donc finalement $p_0 = 3$.

Donc $N = 3 \times 2^2 = 12$ est le seul entier positif tq $\sigma_0(N) = 6$ et $\sigma_1(N) = 28$

$\boxed{\text{Ex } 16}$ On regarde les restes de n^5 modulo 3 et 5 :

$n \equiv 0\ [3] \Rightarrow n^5 \equiv 0\ [3]$
$n \equiv 1\ [3] \Rightarrow n^5 \equiv 1\ [3]$
$n \equiv -1\ [3] \Rightarrow n^5 \equiv -1\ [3]$

et $n \equiv 0\ [5] \Rightarrow n^5 \equiv 0\ [5]$
$n \equiv 1\ [5] \Rightarrow n^5 \equiv 1\ [5]$
$n \equiv 2\ [5] \Rightarrow n^5 \equiv 32 \equiv 2\ [5]$
$n \equiv -1,\ n \equiv -2 \Rightarrow n^5 \equiv n\ [5]$

dans tous les cas, $n^5 - n \equiv 0\ [3]$ et $n^5 - n \equiv 0\ [5]$

donc 3 et 5 divisent $n^5 - n$
$\Rightarrow 15$ divise $n^5 - n$.