1. **Exercice 1b :** Soit $n \in \mathbb{N}$.

   $2^4 \equiv -1$ [17], donc $2^6 \equiv -4$ [17] ou encore $2^6 \equiv 13$ [17].

   On obtient ainsi, $2^{6n} \equiv 13^n$ [17], puis $2^{6n+3} \equiv 8 \times 13^n$ [17].

   $3^4 \equiv 13$ [17], donc $3^{4n} \equiv 13^n$ [17] puis $3^{4n+2} \equiv 9 \times 13^n$ [17].

   Par conséquent, $2^{6n+3} + 3^{4n+2} \equiv (8+9) \times 13^n$ [17], ce qui donne $2^{6n+3} + 3^{4n+2} \equiv 0$ [17] .

   $\boxed{17 \text{ divise } 2^{6n+3} + 3^{4n+2}}$

---

2. **Exercice 1f :** $p^2 - 1 = (p-1)(p+1)$.

   p est un nombre premier différent de 2, donc p est impair.
   $p-1$ et $p+1$ sont deux **entiers pairs consécutifs** : l'un est divisible par 2 et l'autre par 4.
   Par conséquent, 8 divise $p^2 - 1$.

   $p-1$, p et $p+1$ sont trois **entiers consécutifs** : l'un des trois entiers est divisible par 3.
   3 divise $(p-1)p(p+1)$.
   Comme p est un nombre premier différent de 3, p et 3 sont premiers entre eux.
   Par le lemme de Gauss, on déduit que 3 divise $(p-1)(p+1)$.

   Les entiers 8 et 3 divisent $(p-1)(p+1)$ et sont premiers entre eux, donc $(p-1)(p+1)$ est divisible par leur produit.

   $\boxed{\text{Ainsi, 24 divise } p^2 - 1}$

---

3. **Exercice 3c :**
   $7^2 \equiv -1$ [10], donc $7^4 \equiv 1$ [10].

   Simplification du problème :
   On a : $7^{7^7} = 4q + r$ où q et r sont respectivement le quotient et le reste de la division euclidienne de 7^{7^7} par 4. On obtient $7^{7^{7^7}} = 7^{4q+r}$.
   Comme $7^{4q} \equiv 1$ [10], il vient : $7^{4q+r} \equiv 7^r$ [10].

   Déterminons la valeur de r :
   $7^2 \equiv 1$ [4] et 7^7 est un nombre impair donc peut s'écrire sous la forme : $7^7 = 2k + 1$.
   $7^{7^7} \equiv 1^k \times 7$ [4], donc $7^{7^7} \equiv 3$ [4].
   Ainsi, $r = 3$.

   $$\begin{aligned} 7^{7^{7^7}} &\equiv 7^3 \text{ [10]} \\ &\equiv -7 \text{ [10]} \\ &\equiv 3 \text{ [10]} \end{aligned}$$

   $\boxed{\text{Le reste de la division euclidienne de } 7^{7^{7^7}} \text{ est le nombre 3}}$

---

4. **Exercice 4 :** par récurrence sur n.

   Soit P_n : $a^{2^n} \equiv 1$ [2^{n+1}].

   $a^2 - 1 = (a-1)(a+1)$ est le produit de deux nombres pairs (car a est impair), donc est divisible par 4.
   Ainsi, $a^2 - 1 \equiv 0$ [2^2].
   P_1 est vraie.

   Soit $n \in \mathbb{N}^*$ tel que P_n soit vraie.
   $a^{2^{n+1}} - 1 = (a^{2^n})^2 - 1 = (a^{2^n} - 1)(a^{2^n} + 1)$.
   Or $a^{2^n} - 1$ est divisible par 2^n (d'après P_n) et $a^{2^n} + 1$ est un nombre pair, donc est divisible par 2.
   Par conséquent, $a^{2^{n+1}} - 1$ est divisible par 2^{n+1}.
   P_{n+1} est vraie.

---

5. **Exercice 7b :** résoudre $7x - 12y = 3$.

• **Recherche d'une solution particulière :**

7 et 12 sont premiers entre eux, on peut commencer par chercher des coefficients (u, v) tels que $7u - 12v = 1$.

$u = 7$ et $v = 4$ conviennent. (*Rque : si on ne trouve pas de solutions évidentes, on peut utiliser l'algorithme d'Euclide pour obtenir des coefficients de Bézout*)

On multiplie par 3 pour obtenir un couple solution de l'équation.

Le couple $(21, 12)$ est une solution de l'équation.

Remarque : on peut détecter d'autres solutions évidentes comme par exemple $(9, 5)$ *ou* $(-3, -2)$

En effet : $9 \times 7 - 5 \times 12 = 63 - 60 = 3$, $-3 \times 7 + 2 \times 12 = 24 - 21 = 3$

• **Analyse :** soit (x, y) un couple solution.

$7x - 12y = 3$

$\quad = 7 \times 21 - 12 \times 12$

D'où $7(x - 21) = 12(y - 12)$.

7 divise $12(y - 12)$ et 7 est premier avec 12, donc d'après le lemme de Gauss, 7 divise $y - 12$.

Il existe donc $k \in \mathbb{Z}$ tel que $y - 12 = 7k$.

On obtient alors $7(x - 21) = 12 \times 7k$, ce qui donne $x - 21 = 12k$.

Ainsi, $x = 12k + 21$ et $y = 7k + 12$.

• **Synthèse :** supposons que $x = 12k + 21$ et $y = 7k + 12$ où $k \in \mathbb{Z}$.

On vérifie aisément que $7x - 12y = 3$.

Ainsi, les solutions de l'équation sont les couples $(12k + 21, 7k + 12)$ avec $k \in \mathbb{Z}$

---

6. **Exercice 8b :**

Analyse : supposons que n soit un entier relatif admettant 3 pour reste dans la division par 6,
5 pour reste dans la division par 8 et 13 pour reste dans la division par 20.

Il existe $x \in \mathbb{Z}$ tel que $n = 6x + 3$.

Il existe $y \in \mathbb{Z}$ tel que $n = 8y + 5$.

Il existe $z \in \mathbb{Z}$ tel que $n = 20z + 13$.

On a alors $6x + 3 = 8y + 5$ (*on tombe que une équation diophantienne linéaire)*

D'où $3x - 4y = 1 = 4 - 3$

Alors $3(x + 1) = 4(y + 1)$.

4 divise $3(x + 1)$ et 4 est premier avec 3, donc 4 divise $x + 1$.

Il existe $k \in \mathbb{R}$ tel que $x + 1 = 4k$.

Il n'y a pas besoin ici de déterminer la forme de y *:* x *et* y *sont des données intermédiaires, l'objectif est de déterminer la forme de* n*.*

On obtient $n = 6x + 3 = 6(4k - 1) + 3 = 24k - 3$.

L'analyse n'est pas terminée : on a obtenu une forme de n *sans tenir compte de l'hypothèse que le reste de la division de* n *par 20 vaut 13.*

$24k - 3 = 20z + 13$ donne $6k = 5z + 4$.

On tombe sur une deuxième équation diophantienne linéaire. On peut suivre la méthode traditionnelle. On peut également utiliser les relations de congruence.

Or $5z \equiv 0$ [5], d'où $6k \equiv 4$ [5], ce qui donne $k \equiv 4$ [5].

Ainsi, il existe $p \in \mathbb{Z}$ tel que $k = 5p + 4$.

Finalement, $n = 24k - 3 = 120p + 93$.

Synthèse : supposons que $n = 120p + 93$ où $p \in \mathbb{Z}$.

120 étant un multiple de 6, 8 et 20, on a :

n	$\equiv$	93	[6]	n	$\equiv$	93	[8]	n	$\equiv$	93	[20]
	$\equiv$	3	[6]		$\equiv$	5	[8]		$\equiv$	13	[20]

---

7. **Exercice 9 :**

Remarque : on va utiliser les résultats suivants au cours de cet exercice

$$\prod_{i=0}^{p} \lambda x_i = \lambda^{p+1} \prod_{i=0}^{p} x_i \quad \text{et} \quad \prod_{i=0}^{p} a^i = a^{\sum_{i=0}^{p} i} = a^{\frac{p(p+1)}{2}}$$

On pose $n = 3^p 5^q$.

D'après le cours (critère de divisibilité avec les valuations), d est un diviseur de n si et seulement si $d = 3^i 5^j$ avec $i \in [\![0, p]\!]$ et $j \in [\![0, q]\!]$.

Le produit P des diviseurs de n est donc égal à :

$$P = \prod_{i=0}^{p} \left(\prod_{j=0}^{q} 3^i 5^j \right) = \prod_{i=0}^{p} \left(3^{i(q+1)} \prod_{j=0}^{q} 5^j \right) = \prod_{i=0}^{p} 3^{i(q+1)} 5^{\frac{q(q+1)}{2}} = 5^{\frac{(p+1)q(q+1)}{2}} \prod_{i=0}^{p} (3^{(q+1)})^i = 5^{\frac{(p+1)q(q+1)}{2}} 3^{\frac{(q+1)p(p+1)}{2}}$$

On en déduit, par unicité de la décomposition en facteurs premiers, que

$$\frac{(p+1)q(q+1)}{2} = 42 \quad \text{et} \quad \frac{(q+1)p(p+1)}{2} = 84$$

D'où $p = 2q$ puis $q = 3$ et $p = 6$.

Ainsi, $n = 3^6 5^3$

---

8. **Exercice 10c : calcul de PGCD**

On note $d = \text{PGCD}(2n^3 - 7n, 2n + 1)$.

• d divise $2n + 1$ et d divise $2n^3 - 7n$, donc d divise $n^2(2n + 1) - (2n^3 - 7n) = n^2 + 7n$.
Puis, d divise $2(n^2 + 7n) - n(2n + 1) = 13n$.
Enfin, d divise $13(2n + 1) - 2 \times 13n = 13$.
Finalement, $d = 1$ ou $d = 13$.

Commentaires :
L'exercice est loin d'être terminé. A ce stade de l'étude, les 3 situations suivantes peuvent avoir lieu :
• quelque soit l'entier n, le PGCD vaut 1
• quelque soit l'entier n, le PGCD vaut 13
• le PGCD vaut 1 pour certaines valeurs de n, et 13 pour d'autres valeurs de n
On peut expérimenter sur quelques valeurs de n pour avoir une idée du résultat.
On s'aperçoit que pour $n = 2$, on a : $\text{PGCD}(2n^3 - 7n, 2n + 1) = \text{PGCD}(2, 5) = 1$
Et pour $n = 6$, on a : $\text{PGCD}(2n^3 - 7n, 2n + 1) = \text{PGCD}(390, 13) = 13$.

Il reste à déterminer une condition nécessaire et suffisante (simple) sur n pour que $d = 13$.

• Recherche d'une condition nécessaire sur n pour que $d = 13$:

Supposons $d = 13$:
Alors 13 divise $2n + 1$, donc $2n + 1 \equiv 0$ [13].
En multipliant par 6, on obtient : $12n + 6 \equiv 0$ [13].
Or $12 \equiv -1$ [13].
On obtient alors : $-n + 6 \equiv 0$ [13].
Ainsi, $n \equiv 6$ [13].

• On vérifie que la condition trouvée est suffisante pour que $d = 13$:

Réciproquement, supposons $n \equiv 6$ [13] :
Alors $2n + 1 \equiv 0$ [13], donc 13 divise $2n + 1$.
Et $n^2 \equiv 36$ [13], donc $n^2 \equiv 10$ [13].
Puis $n^3 \equiv 60$ [13], soit $n^3 \equiv 8$ [13], par conséquent, $2n^3 \equiv 3$ [13].
Et $7n \equiv 42$ [13], donc $7n \equiv 3$ [13].
Ainsi, $2n^3 - 7n \equiv 0$ [13] : 13 divise $2n^3 - 7n$.

Conclusion : $\text{PGCD}(2n^3 - 7n, 2n + 1) = 13$ si et seulement si $n \equiv 6$ [13]
$\text{PGCD}(2n^3 - 7n, 2n + 1) = 1$ si et seulement si $n \not\equiv 6$ [13].

---

9. **Exercice 11a :**

Soit $(x, y) \in \mathbb{Z}^{*2}$. On a les équivalences suivantes :

$$\begin{aligned}
\frac{1}{x}+\frac{1}{y}=\frac{1}{5} &\iff 5(y+x)=xy \\
&\iff 5(y+x)=yy \\
&\iff xy-5x-5y=0 \\
&\iff (x-5)(y-5)=25 \\
&\iff \left\{\begin{array}{l} x-5=-25 \\ y-5=-1 \end{array}\right. \textbf{ ou } \left\{\begin{array}{l} x-5=-5 \\ y-5=-5 \end{array}\right. \textbf{ ou } \left\{\begin{array}{l} x-5=-1 \\ y-5=-25 \end{array}\right. \\
&\qquad \textbf{ou } \left\{\begin{array}{l} x-5=25 \\ y-5=1 \end{array}\right. \textbf{ ou } \left\{\begin{array}{l} x-5=5 \\ y-5=5 \end{array}\right. \textbf{ ou } \left\{\begin{array}{l} x-5=1 \\ y-5=25 \end{array}\right. \\
&\iff \left\{\begin{array}{l} x=-20 \\ y=4 \end{array}\right. \textbf{ ou } \left\{\begin{array}{l} x=0 \\ y=0 \end{array}\right. \text{ (exclu) } \textbf{ou } \left\{\begin{array}{l} x=4 \\ y=-20 \end{array}\right. \textbf{ ou } \left\{\begin{array}{l} x=30 \\ y=6 \end{array}\right. \\
&\qquad \textbf{ou } \left\{\begin{array}{l} x=10 \\ y=10 \end{array}\right. \textbf{ ou } \left\{\begin{array}{l} x=6 \\ y=30 \end{array}\right.
\end{aligned}$$

Ainsi, les solutions de l'équation sont les couples $(-20, 4)$, $(4, -20)$, $(10, 10)$, $(30, 6)$ et $(6, 30)$.

Ainsi, l'ensemble des solutions est $\mathcal{S} = \{ (-20, 4), (4, -20), (10, 10), (30, 6) , (6, 30) \}$

---

10. **Exercice 11c :**

Analyse : soit (x, y) un couple solution.
Alors $x^2 - y^2 - 4x - 2y = 5$.
Or $(x-2)^2 = x^2 - 4x + 4$ et $(y+1)^2 = y^2 + 2y + 1$.
D'où $(x-2)^2 - (y+1)^2 = 8$, puis $(x - y - 3)(x + y - 1) = 8$.
Donc $x - y - 3$ et $x + y - 1$ sont des diviseurs de 8.
Il existe $a \in D(8)$ et $b \in D(8)$ tels que

$$\left\{\begin{array}{l} x-y+3=a \\ x+y-1=b \\ ab=8 \end{array}\right.$$

Ce qui donne :

$$\left\{\begin{array}{l} x=\frac{a+b}{2}+2 \\ y=\frac{b-a}{2}-1 \\ ab=8 \end{array}\right.$$

Parmi les couples (a, b) de diviseurs de 8 possibles, seuls les couples $(4, 2)$, $(2, 4)$, $(-4, -2)$ et $(-4, -2)$ conduisent à des solutions x et y entières.
On obtient $(x, y) = (5, 0)$ ou $(x, y) = (5, -2)$ ou $(x, y) = (-1, 0)$ ou $(x, y) = (-1, -2)$.

Synthèse : on vérifie sans difficulté que les 4 couples trouvés sont bien solutions de l'équation.

---

11. **Exercice 11e :**

Analyse : Soit (x, y) un couple solution.
$4y^3 \leq 3x^3 + xy + 4y^3 = 349 < 4 \times 5^3$.
On en déduit que $y < 5$.
De même $3x^3 \leq 3x^3 + xy + 4y^3 = 349 < 3 \times 5^3$. Donc $x < 5$.

Synthèse :
On évalue l'expression $3x^3 + xy + 4y^3$ pour les 25 couples possibles (x, y) avec $x \in [\![0, 4]\!]$ et $y \in [\![0, 4]\!]$,
et on trouve que (x, y) est solution de l'équation si et seulement si $(x, y) = (3, 4)$.

---

12. **Exercice 20 :**

Soit $(a,b,c,d) \in \mathbb{Z}^4$ tel que $a \wedge b = 1$ et $c \wedge d = 1$.

Notons $p = ac \wedge bd$, $p' = a \wedge d$ et $p'' = c \wedge b$.

Méthode : *p et $p'p''$ sont tous deux positifs. Pour prouver que $p = p'p''$, il suffit de montrer que p divise $p'p''$ et que $p'p''$ divise p.*

- p' divise a, donc divise ac.

Et p' divise d, donc divise bd.
Par conséquent, **p' divise p.**

De même, **p'' divise p.**

$p' \wedge p''$ divise p', donc divise a,
Et $p' \wedge p''$ divise p'' donc divise b.
Par conséquent, $p' \wedge p''$ divise $a \wedge b = 1$.
p' et p'' sont premiers entre eux.

On en déduit que $p'p''$ divise p

- Il existe $(u,v) \in \mathbb{Z}^2$ et $(u',v') \in \mathbb{Z}^2$ tels que $p' = au + dv$ et $p'' = bu' + cv'$.

On a alors $p'p'' = abX_1 + acX_2 + bdX_3 + cdX_4$ avec $\begin{cases} X_1 = uu' \\ X_2 = uv' \\ X_3 = vu' \\ X_4 = vv' \end{cases}$

Or p divise ac et p divise bd.
Il reste à prouver que p divise ab et cd pour obtenir que p divise (par combinaison linéaire) $p'p''$.

D'après le théorème de Bézout, il existe (u'',v'') tel que $au'' + bv'' = 1$.
On multiplie par cd, et on obtient $acdu'' + bcdv'' = cd$.
Comme p divise ac et p divise bd, alors p divise $acdu'' + bcdv'' = cd$.

On montre par un raisonnement similaire que p divise ab.

Ainsi, p divise $p'p''$

---

13. **Exercice 27 : épreuve orale X MP**

Notons $k = v_2(n)$.
Il existe $p \in \mathbb{N}^*$ premier avec 2 tel que $n = 2^k p$.
p est donc un nombre impair.
On a alors :

$$a^n + b^n = (a^{2^k})^p - (-b^{2^k})^p = (a^{2^k} + b^{2^k}) \times \sum_{i=0}^{p-1} (a^{2^k})^i (b^{2^k})^{p-1-i}$$

Donc $a^{2^k} + b^{2^k}$ est un diviseur de $a^n + b^n$.
Or $a^n + b^n$ est un nombre premier, donc $a^{2^k} + b^{2^k} = 1$ ou $a^{2^k} + b^{2^k} = a^n + b^n$.
Comme $a^{2^k} + b^{2^k} \geq 2$, on en déduit que $a^{2^k} + b^{2^k} = a^n + b^n$.

Comme $2^k \leq n$, on a $a^{2^k} \leq a^n$ et $b^{2^k} \leq b^n$.
Ainsi, l'égalité $a^{2^k} + b^{2^k} = a^n + b^n$ entraîne $a^{2^k} = a^n$ et $b^{2^k} = b^n$.
$a \geq 2$, on déduit que $2^k = n$.

n est une puissance de 2

Exemple : $2^4 + 3^4$, $2^4 + 5^4$, $2^8 + 13^8$ sont des nombres premiers.

---

14. **Exercice 28 :**

L'implication $\Longrightarrow$ est démontrée dans le cours.

$\Longleftarrow$: supposons que n soit composé.

Soit p un diviseur premier de n : il existe $q \in \mathbb{N}$ tel que $n = pq$.

Supposons par l'absurde que n divise $\binom{n}{p}$.

$\frac{1}{n}\binom{n}{p}$ est donc un entier. Or $\frac{1}{n}\binom{n}{p} = \frac{1}{p}\binom{n-1}{p-1}$

On en déduit que p divise $\binom{n-1}{p-1} = \frac{(n-1)(n-2)\cdots(n-p+1)}{(p-1)!}$

Comme p est premier, il divise donc l'un des facteurs du produit $(n-1)(n-2)\cdots(n-p+1)$.

Notons $(n-i)$ le facteur que p divise (i est un entier compris entre 1 et $p-1$).

p divise n et p divise $n-i$, donc p divise i.

Par conséquent, $p \leq i$ ce qui est contradictoire avec $i \leq p-1$.

---

15. **Exercice 32 :**

Soit $a \in [\![1, n-1]\!]$.

Notons $d = a \wedge n$.

d divise n et n divise $a^{n-1} - 1$, donc par transitivité, d divise $a^{n-1} - 1$.

De plus, d divise a donc d divise a^{n-1}.

Par conséquent, d divise $a^{n-1} - (a^{n-1} - 1)$, c'est-à-dire d divise 1, et donc $d = 1$.

Ainsi, n est premier avec tout entier $a \in [\![1, n-1]\!]$.

On en déduit que n est premier

---

16. **Exercice 34 :**

a) On note $d = x \wedge y$.

Il existe $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $\begin{cases} x = da \\ y = db \\ a \wedge b = 1 \end{cases}$

Comme $x \leq y$, on a : $a \leq b$.

On a : $x^y = y^x$, ce qui donne $(x^b)^d = (y^a)^d$.

La fonction $t \mapsto t^d$ étant injective sur $\mathbb{R}_+$, on en déduit que : $x^b = y^a$.

D'où $d^b a^b = d^a b^a$, puis $d^{b-a} a^b = b^a \quad (*)$

On en déduit que a divise b^a.

Comme de plus, a est premier avec b, donc avec b^a, on obtient par le lemme de Gauss que a divise 1.

Par conséquent, $a = 1$

$x = d$ **est donc un diviseur de** y**.**

b) $(*)$ donne alors $d^{b-1} = b$.

On distingue 2 cas :

- **On suppose $b \geq 2$:**

Alors $d \times d^{b-2} = b$, donc d divise b et par conséquent $d \leq b$.

De plus, $b = d^{b-1} \geq d^{2-1} = d$.

On obtient ainsi $b = d$.

Puis $b^{b-1} = b$, ce qui donne $b = 2$ et donc $d = 2$.

Ainsi, $x = da = 2$ et $y = db = 4$.

- **On suppose $b = 1$:**

Alors $x = y$.

Réciproquement, il est immédiat que les couples $(2, 4)$, $(4, 2)$ et (x, x) (avec $x \in \mathbb{N}^*$) sont solutions de l'équation.

Ainsi, l'ensemble $\mathcal{S}$ des solutions de l'équation est : $\mathcal{S} = \{(2, 4), (4, 2)\} \cup \{(x, x) \mid x \in \mathbb{N}^*\}$

---

17. **Exercice 39 :**

On suppose par l'absurde qu'il n'existe qu'un nombre fini de nombre premiers de cette forme, notés p_1, p_2, ..., p_k.

On considère alors $N = 4p_1p_2...p_k - 1$.
N est impair donc 2 ne divise pas N.
Les facteurs premiers de N sont des nombres impairs, donc sont congrus à 1 ou à 3 modulo 4.
Si tous les facteurs premiers sont congrus à 1 modulo 4, alors $N \equiv 1 \ [4]$, ce qui est contradictoire avec $N \equiv -1 \ [4]$.
Par conséquent, l'un au moins des facteurs premiers de N est égal à 3 modulo 4, donc est de la forme $4q + 3$, c'est donc l'un des p_i (où $1 \leq i \leq k$).
p_i divise N et p_i divise $4p_1p_2...p_k$, donc p_i divise 1. Contradiction.