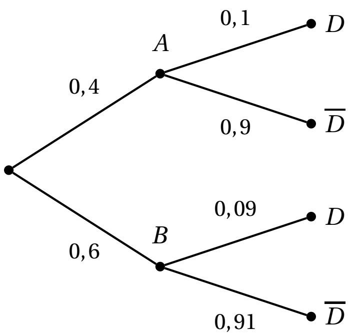
Correction du contrôle commun n° 4

Exercice 1 (5 points)

1. (a)



(b) On demande $p(A\cap D)$.
$p(\mathrm{A}\cap\mathrm{D}) = p_{\mathrm{D}}(\mathrm{A}) \times p(\mathrm{A}) = 0,4\times 0,1$, donc
$p(\mathrm{A}\cap\mathrm{D}) = \boxed{0,04}$.

(c) On calcule aussi $p(\mathrm{B}\cap\mathrm{B})$ de la même façon, c'est $0,6\times 0,09 = \boxed{0,054}$.
A et B sont des évènements formant une partition de l'ensemble des pièces (c'est-à-dire
D = (D∩A)∪(D∩B) et c'est une réunion d'évènements disjoints),.
Alors : $P(\mathrm{D}) = p(\mathrm{D}\cap(\mathrm{A}\cup\mathrm{B}))$
$p(\mathrm{D}) = p((\mathrm{D}\cap\mathrm{A})\cup(\mathrm{D}\cap\mathrm{B})) = p(\mathrm{D}\cap\mathrm{A}) + p(\mathrm{D}\cap\mathrm{B})$
$= p_{\mathrm{A}}(\mathrm{D})\times p(\mathrm{A}) + p_{\mathrm{B}}(\mathrm{D})\times p(\mathrm{B})$ (formule des probabilités totales).
Ainsi :
$p(\mathrm{D}) = 0,04 + 0,054 = \boxed{0,094}$.

(d) On nous demande $p_{\mathrm{D}}(\mathrm{A})$, on utilise la formule :
$p_{\mathrm{D}}(\mathrm{A}) = \dfrac{p(\mathrm{D}\cap\mathrm{A})}{p(\mathrm{D})} = \dfrac{0,04}{0,094} = \dfrac{40}{94} = \boxed{\dfrac{20}{47}}$.

2. (a) On a répétition de 150 expériences **identiques** et **indépendantes** avec **deux** issues :
X suit donc la loi binomiale de paramètres $n = 150$ et $p = 0,1$: $\boxed{X \hookrightarrow \mathscr{B}(150\,;\,0,1)}$.

(b) Pour tout k entier compris entre 0 et 150, on a
$p(X = k) = \dbinom{n}{k} p^k (1-p)^{n-k}$ donc

$$\boxed{p(X = k) = \binom{150}{k}\times 0,1^k \times 0,9^{150-k}}.$$

On demande $p(X \leqslant 1)$.
$p(X \leqslant 1) = p(X = 0) + p(X = 1)$
$= 0,9^{150} + 150\times 0,1\times 0,9^{149} \approx \boxed{2,4610^{-6}}$

(c) $p(X \leqslant 149) = 1 - p(X = 150)$
$= 1 - \dbinom{150}{0}\times 0,1^0 \times 0,9^150 = \boxed{1-10^{-150}}$ (valeur exacte). (remarque : la calculatrice affiche 1, mais cet événement **n'est pas certain**)

3. $p(X \geqslant 1) = 1 - p(X = 0) = 1 - \dbinom{n}{0}\times 0,1^0 \times 0,9^n = 1 - 0,9^n$.
On cherche n tel que $1 - 0,9^n \geqslant 0,99$.
$1 - 0,9^n \geqslant 0,99 \iff 1 - 0,99 \leqslant 0,9^n \iff 0,01 \leqslant 0,9^n$
$\iff \ln(0,01) \leqslant n\ln(0,9) \iff n \geqslant \dfrac{\ln(0,01)}{\ln(0,9)} \approx 43,7$.
Le plus petit entier tel que $p(X \geqslant 1) \geqslant 0,99$ est $\boxed{n = 44}$.

Exercice 2 (5 points)

Partie A :

1. Soient n et p deux naturels distincts.
$f_n(x) = f_p(x) \iff \dfrac{\mathrm{e}^{-nx}}{1+\mathrm{e}^{-x}} = \dfrac{\mathrm{e}^{-px}}{1+\mathrm{e}^{-x}}$
$\iff \mathrm{e}^{-nx} = \mathrm{e}^{-px}$ (car $1+\mathrm{e}^{-x} > 0$)
$\iff -nx = -px$ (par croissance de la fonction ln)
$\iff \boxed{x = 0}$ (car $n \neq p$).
Quel que soit $n\in\mathbb{N}$, $f_n(0) = \dfrac{\mathrm{e}^0}{1+\mathrm{e}^0} = \dfrac{1}{2}$.
Toutes les courbes $\mathscr{C}_n$ passent par le point $\left(0\,,\,\dfrac{1}{2}\right)$ et ont ce point pour seul point commun.

2. Étude de la fonction f_0

(a) $f_0(x) = \dfrac{1}{1+\mathrm{e}^{-x}}$.
Cette fonction est dérivable sur $\mathbb{R}$ et
$f_0'(x) = -\dfrac{-\mathrm{e}^{-x}}{(1+\mathrm{e}^{-x})^2} = \boxed{\dfrac{\mathrm{e}^{-x}}{(1+\mathrm{e}^{-x})^2}}$.
Comme $\mathrm{e}^{-x} > 0$ et $\left(1+\mathrm{e}^{-x}\right)^2 >$, on en déduit que $\boxed{f_0'(x) > 0}$.
La fonction f_0 est donc **croissante** sur $\mathbb{R}$.

(b) On sait que $\displaystyle\lim_{x\to-\infty} \mathrm{e}^x = 0$. Donc $\boxed{\displaystyle\lim_{x\to-\infty} \mathrm{e}^{-x} = +\infty}$.
Donc $\boxed{\displaystyle\lim_{x\to-\infty} f_n(x) = 0}$. Ceci signifie que l'axe des abscisses est **asymptote** à la courbe $\mathscr{C}_0$ au voisinage de $-\infty$.
On sait que $\displaystyle\lim_{x\to+\infty} \mathrm{e}^{-x} = 0$, donc $\boxed{\displaystyle\lim_{x\to+\infty} f_0(x) = 1}$.
Ceci signifie que la droite d'équation $y = 1$ est **asymptote** horizontale à la courbe $\mathscr{C}_0$ au voisinage de $+\infty$.

(c)

x	$-\infty$	$+\infty$
$f(x)$	0	1

3. Étude de la fonction f_1

(a) On a $f_1(x) = \dfrac{\mathrm{e}^{-x}}{1+\mathrm{e}^{-x}} = \dfrac{1}{\mathrm{e}^x+1}$ en multipliant numérateur et dénominateur par e^x.

- $\lim\limits_{x\to-\infty} e^x = 0$ donc $\boxed{\lim\limits_{x\to-\infty} f_1(x) = 1}$.
- $f_1(x) = \dfrac{e^{-x}}{1+e^{-x}}$; $\lim\limits_{x\to+\infty} (-x) = -\infty$ donc $\lim\limits_{x\to+\infty} e^{-x} = \lim\limits_{X\to-\infty} e^X = 0$, d'où $\boxed{\lim\limits_{x\to+\infty} f_1(x) = 0}$
- $f_1(x) = \dfrac{1}{1+e^x} = \dfrac{1}{u(x)}$ avec $u(x) = 1+e^x$.
  $f_1' = \left(\dfrac{1}{u}\right)' = -\dfrac{u'}{u^2}$ avec $u'(x) = e^x$.
  Alors $\boxed{f_1'(x) = -\dfrac{e^x}{(1+e^x)^2} < 0}$ car $e^x > 0$ donc f_1 est décroissante.
  Tableau de variation :

x	$-\infty$		$+\infty$
$f_1(x)$	1	$\searrow$	0

4. Étude de la fonction f_n pour $n \geqslant 2$
   (a) $f_n(x) = \dfrac{e^{-nx}}{1+e^{-x}}$. En multipliant chaque terme par $e^{nx} > 0$, $\boxed{f_n(x) = \dfrac{1}{e^{nx}+e^{(n-1)x}}}$.
   (b) Pour $p \geqslant 2$, $\lim\limits_{x\to+\infty} e^{px} = +\infty$, donc en utilisant l'écriture du **a.**, $\boxed{\lim\limits_{x\to+\infty} f_n(x) = 0}$.
   Limite en $-\infty$: $\lim\limits_{x\to-\infty} e^{nx} = 0_+$ et $\lim\limits_{x\to-\infty} e^{(n-1)x} = 0_+$ donc par limite de l'inverse $\boxed{\lim\limits_{x\to+\infty} e^{-x} = +\infty}$
   (c) f_n quotient de sommes de fonctions dérivables est dérivable car $e^{nx}+e^{(n-1)x} > 0$.
   En utilisant l'écriture trouvée au début de la question :
   $\boxed{f_n'(x) = -\dfrac{ne^{nx}+(n-1)e^{(n-1)x}}{\left(e^{nx}+e^{(n-1)x}\right)^2}}$.
   Comme $n \geqslant 2$, cette dérivée est **négative** quel que soit x réel. Les fonctions $(f_n,\ n \geqslant 2)$ sont donc **décroissantes** de $+\infty$ à 0.

Partie B : *Étude d'une suite liée aux fonctions f_n*

1. $u_1 = \displaystyle\int_0^1 f_1(x)\,dx = \int_0^1 \frac{e^{-x}}{1+e^{-x}}\,dx$.
   En posant $u(x) = 1+e^{-x}$, $u'(x) = -e^{-x}$, on remarque que la fonction à intégrer est $-\dfrac{u'(x)}{u(x)}$ dont une primitive est la fonction $-\ln\left(1+e^{-x}\right)$.
   Donc $u_1 = \left[-\ln\left(1+e^{-x}\right)\right]_0^1 = \boxed{-\ln\left(1+e^{-1}\right)+\ln 2}$.
   Par linéarité, on a :
   $u_0+u_1 = \displaystyle\int_0^1 \frac{1}{1+e^{-x}}\,dx + \int_0^1 \frac{e^{-x}}{1+-x}\,dx = \int_0^1 \frac{1+e^{-x}}{1+e^{-x}\,dx}$
   $= \displaystyle\int_0^1 1\,dx = \boxed{1}$.
   On en déduit $u_0+u_1 = 1$ donc
   $$u_0 = 1-u_1 = \boxed{1-\ln 2+\ln\left(1+e^{-1}\right)}.$$
2. On a la suite d'inéquations :
   $e^{-x} > 0 \iff 1+e^{-x} > 1 \iff 0 < \dfrac{1}{1+e^{-x}} < 1$
   $\iff 0 < \dfrac{e^{-nx}}{1+e^{-x}} < e^{-nx}$ donc $\boxed{0 \leqslant f_n(x) \leqslant e^{-nx}}$.
   En intégrant ces trois fonctions sur $[0\,;\,1]$, on trouve, par **conservation de l'ordre** :
   $0 < \displaystyle\int_0^1 \frac{e^{-nx}}{1+e^{-x}}\,dx < \int_0^1 e^{-nx}\,dx \iff 0 < u_n < \int_0^1 e^{-nx}\,dx$.
3. $\displaystyle\int_0^1 e^{-nx}\,dx = \left[-\frac{1}{n}e^{-nx}\right]_0^1 = -\frac{1}{n}\left(e^{-n}-1\right) = \frac{1}{n}\left(1-e^{-n}\right)$.
   Par limite au voisinage de $+\infty$:
   $\lim\limits_{x\to+\infty} e^{-n} = 0$, $\lim\limits_{x\to+\infty} 1-e^{-n} = 1$, $\lim\limits_{x\to+\infty} \dfrac{1}{n} = 0$, donc par produit :
   $\lim\limits_{x\to+\infty} \dfrac{1}{n}\left(1-e^{-n}\right) = 0$.
   En utilisant l'encadrement de la question **2.**, et d'après le théorème des « gendarmes », on obtient
   $\boxed{\lim\limits_{x\to+\infty} u_n = 0}$.
   La suite est donc convergente. vers 0

Exercice 3 (5 points)

Restitution organisée de connaissances
voir cours

Les deux parties peuvent être traitées indépendamment.
Partie A

1. $z^2-2z+2 = 0$ a pour discriminant $\Delta = -4 < 0$.
   L'équation a deux solutions complexes conjuguées : $\boxed{z_1 = 1-i}$ et $\boxed{z_2 = \overline{z_1} = 1+i}$.
2. Soit M_1 d'affixe $z_1 = 1-i$.
   On a $AM_1 = |z_1-z_A| = |1-i-1| = |-i| = \boxed{1}$.
   De même $AM_2 = |z_2-z_A| = |1+i-1| = |i| = \boxed{1}$.
   Ces deux résultats signifient que M_1 et M_2 appartiennent au cercle de centre A et de rayon 1 soit au cercle $\mathscr{C}$.

Partie B

1. Figure : voir à la fin de l'exercice.
2. $z' = \dfrac{2z-1}{2z-2} \Rightarrow z'-1 = \dfrac{2z-1}{2z-2}-1 \iff z'-1 = \dfrac{2z-1-2z+2}{2z-2}$
   $\iff z"-1 = \dfrac{1}{2(z-1)} \iff \boxed{\left(z'-1\right)(z-1) = \dfrac{1}{2}}$.

3. Le résultat précédent entraîne :

   - en termes de modules : $\boxed{AM \times AM' = \dfrac{1}{2}}$;
   - le produit des deux complexes étant non nul aucun des deux facteurs ne peut l'être, et en particulier $z'-1 \neq 0 \iff z' \neq 1$, soit $\boxed{M' \neq \mathrm{A}}$;
   - en termes d'argument : $\arg\left[\left(z'-1\right)(z-1)\right] = 0 + 2k\pi$. Or $\arg\left[\left(z'-1\right)(z-1)\right] = \left(\vec{u}\,;\,\overrightarrow{\mathrm{AM}}\right) + \left(\vec{u}\,;\,\overrightarrow{\mathrm{AM'}}\right)$, donc

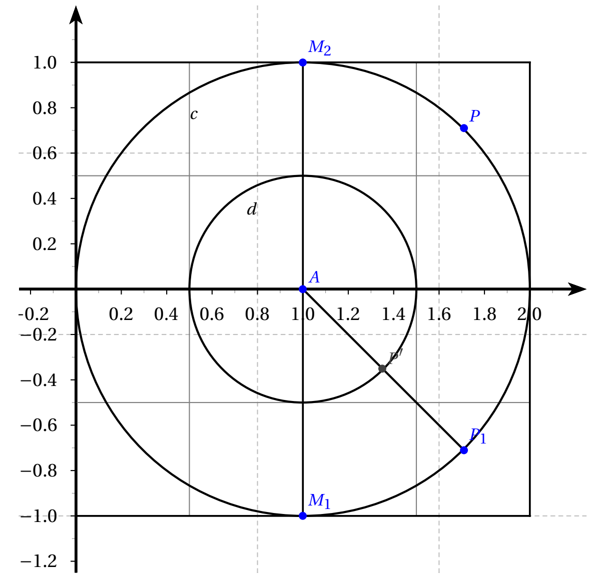
   $\boxed{\left(\vec{u}\,;\,\overrightarrow{\mathrm{AM}}\right) + \left(\vec{u}\,;\,\overrightarrow{\mathrm{AM'}}\right) = 0 + 2k\pi, \text{ où } k \text{ est un entier relatif}}$.

4. On a $z_{\mathrm{P}} = 1 + \mathrm{e}^{\mathrm{i}\frac{\pi}{4}} \iff z_{\mathrm{P}} - 1 = \mathrm{e}^{\mathrm{i}\frac{\pi}{4}} \Rightarrow \left|z_{\mathrm{P}} - 1\right| = \left|\mathrm{e}^{\mathrm{i}\frac{\pi}{4}}\right|$
   $\iff \left|z_{\mathrm{P}} - 1\right| = \boxed{1}$.
   Cette dernière égalité montre que P appartient au cercle de centre A et de rayon 1, donc au cercle $\mathscr{C}$.
   Il ne reste plus qu'à construire sur ce cercle le point tel que $\left(\vec{u}\,,\,\overrightarrow{\mathrm{AP}}\right) = \dfrac{\pi}{4}$.

5. On a AP $\times$AP$' = \dfrac{1}{2}$; or AP $= 1$, donc $\boxed{\mathrm{AP}' = \dfrac{1}{2}}$.le point P$'$ appartient au cercle $\mathscr{C}_1$ de centre A et de rayon $\dfrac{1}{2}$.
   D'autre part on a $\left(\vec{u}\,,\,\overrightarrow{\mathrm{AP'}}\right) = -\dfrac{\pi}{4}$.
   On peut donc construire P$_1$ symétrique sur le cercle $\mathscr{C}$ du point P autour de l'axe horizontal contenant A. Le point P$'$ est le point commun à [AP$_1$] et au cercle $\mathscr{C}_1$. Voir Figure.

6. (a) On a donc $z = \dfrac{3}{4} + \mathrm{i}t$ avec $t \in \mathbb{R}$.
   Or : $(z'-1)(z-1) = \dfrac{1}{2}$ donc $z' - 1 = \dfrac{1}{2(z-1)}$ donc
   $z' = 1 + \dfrac{1}{2(z-1)} = 1 + \dfrac{1}{2\left(\frac{3}{4} + \mathrm{i}t - 1\right)} = 1 + \dfrac{1}{2\left(-\frac{1}{4} + \mathrm{i}t\right)}$
   $= 1 + \dfrac{1}{2\left(\dfrac{-1+4\mathrm{i}t}{4}\right)} = 1 + \dfrac{1}{\dfrac{-1+4\mathrm{i}t}{2}} = 1 + \dfrac{2}{-1+4\mathrm{i}t}$
   $= \dfrac{-1+4\mathrm{i}t}{-1+4\mathrm{i}t} = \boxed{\dfrac{1+4\mathrm{i}t}{-1+4\mathrm{i}t}}$.
   On en déduit : $z' = \left|\dfrac{1+4\mathrm{i}t}{-1+4\mathrm{i}t}\right| = \dfrac{|1+4\mathrm{i}t|}{|-1+4\mathrm{i}t|}$
   $= \dfrac{\sqrt{(1)^2+(4t)^2}}{\sqrt{(-1)^2+(4t)^2}} = 1$ donc $\boxed{\left|z'\right| = 1}$
   Le point M" appartient au cercle $\mathscr{C}'$ de centre O de rayon 1.

   (b) Un point M' de $\mathscr{C}'$ a une affixe qui peut s'écrire $z' = \mathrm{e}^{\mathrm{i}a}$ avec $a \in \mathbb{R}$. Son ou ses antécédents par f vérifient :
   $\mathrm{e}^{\mathrm{i}a} = \dfrac{2z-1}{2z-2} \iff 2z\mathrm{e}^{\mathrm{i}a} - 2\mathrm{e}^{\mathrm{i}a} = 2z - 1 \iff$
   $2z\left(\mathrm{e}^{\mathrm{i}a} - 1\right) = 2\mathrm{e}^{\mathrm{i}a} - 1 \iff z = \dfrac{2\mathrm{e}^{\mathrm{i}a} - 1}{\mathrm{e}^{\mathrm{i}a} - 1}$ si $\mathrm{e}^{\mathrm{i}a} - 1 \neq 0$.
   Or $\mathrm{e}^{\mathrm{i}a} - 1 = 0 \iff \mathrm{e}^{\mathrm{i}a} = 1 \iff a = 0 \iff z = 1$.
   C'est le point A et on sait que ce point n'a pas d'image par f. La réponse est : **non**.



Exercice 4 (5 points)

Pour les élèves n'ayant pas suivi l'enseignement de spécialité

Partie A

$$f(x) = x - \ln\left(x^2+1\right).$$

1. $f(x) = x \iff x - \ln\left(x^2+1\right) = x \iff \ln\left(x^2+1\right) = 0$
   $\iff x^2 + 1 = 1 \iff x^2 = 0 \iff \boxed{x = 0}$
2. f somme de fonctions dérivables sur $[0\,;\,1]$ est dérivable et sur cet intervalle :
   $f'(x) = 1 - 2x \times \dfrac{1}{x^2+1} = \dfrac{x^2+1-2x}{x^2+1} = \boxed{\dfrac{(x-1)^2}{x^2+1}}$.
   On a quel que soit x, $x^2+1 \geqslant 1 > 0$ et sur $[0\,;1]$, $(x-1)^2 \geqslant 0$, donc sur $[0\,;1]$, $f'(x) \geqslant 0$: la fonction est donc **croissante** sur $[0\,;1]$.
   On a vu que $f(0) = 0$ et $f(1) = \boxed{1 - \ln 2 < 1}$. La fonction est croissante de 0 à $1 - \ln 2 < 1$, donc toutes les images $f(x)$ appartiennent à l'intervalle $[0\,;1]$.

x	0	1
$f(x)$	0 $\nearrow$	$1 - \ln 2 < 1$

Partie B

1. Figure à la fin de l'exercice (Annexe exercice IV)
2. On effectue une **démonstration par récurrence** :
   Initialisation : $u_0 = 1 \leqslant 1$, donc $u_0 \in [0\,;\,1]$.
   Hérédité : Supposons qu'il existe un entier p tel que $u_p \in [0\,;\,1]$; d'aprËs la partie A, on a $u_{p+1} = f\left(u_p\right)$ et on a vu que si $u_p \in [0\,;\,1]$, alors
   $\boxed{f\left(u_p\right) = u_{p+1} \in [0\,;\,1]}$.

D'après l'axiome de récurrence, la propriété est vraie pour tout $n \in \mathbb{N}$.

On a donc pour tout naturel n, $u_n \in [0~;~1]$.

3. Pour tout $n \in \mathbb{N}$, $u_{n+1} - u_n = \boxed{-\ln\left(u_n^2+1\right)}$

   Or $u_n \geqslant 0 \Rightarrow u_n^2 \geqslant 0 \Rightarrow u_n^2+1 \geqslant 1 \Rightarrow \ln\left(u_n^2+1\right) \geqslant 0$
   $\iff 0 \geqslant -\ln\left(u_n^2+1\right)$.

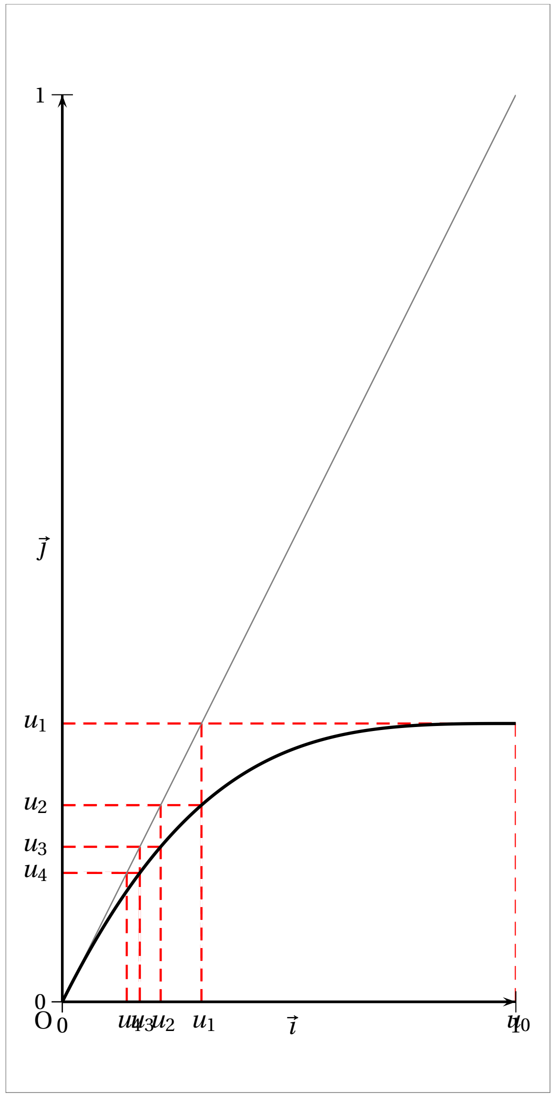
   Conclusion : quel que soit le naturel n, $\boxed{u_{n+1}-u_n \leqslant 0}$: la suite est **décroissante**.

4. La suite est décroissante et tous ses termes sont minorés par 0 : elle est donc **convergente** vers une limite supérieure ou égale à 0.

   f est continue, donc la limite ℓ est solution de l'équation $f(x) = x$. La seule solution est 0 (d'après A.1.) donc $\boxed{\ell = 0}$.

   On a donc $\boxed{\displaystyle\lim_{n\to+\infty} u_n = 0}$.

Annexe à l'exercice IV



Exercice 4 de spécialité (5 points)

Pour les élèves ayant suivi l'enseignement de spécialité

Partie A. Quelques exemples

1. $4 \equiv 1 \mod 3$, donc $4^n \equiv 1^n \mod 3$ et finalement $\boxed{4^n \equiv 1 \mod 3}$.
2. 4 est premier avec 29 (29 est premier). Donc d'après le petit théorème de Fermat $\boxed{4^{29-1} - 1 \equiv 0 \mod 29}$ donc $4^{28} - 1$ est divisible par 28.
3. $4 = 0 \times 17 + 4$;
   $4^2 = 0 \times 17 + 16$;
   $4^3 = 3 \times 17 + 13$;
   $4^4 = 15 \times 17 + 1$.

   La dernière égalité montre que $\boxed{4^4 \equiv 1 \mod 17}$, d'où $\boxed{\left(4^4\right)^k \equiv 1^k \mod 17}$ soit $4^{4k} \equiv 1 \mod 17$ ou encore $4^{4k} - 1 \equiv 0 \mod 17$.

   Conclusion : $\boxed{4^{4k} - 1 \text{ est divisible par } 17}$.
4. On a $4^2 = 16 = 3 \times 5 + 1$ ou $4^2 \equiv 1 \mod 5$ d'où il résulte que $4^{2k} \equiv 1 \mod 5$ ou encore $\boxed{4^{2k} - 1 \equiv 0 \mod 5}$.
   Conclusion : $4^n - 1$ est divisible par 5 si n est pair.

   En revanche : de $4 \equiv 4 \mod 5$ et $4^{2k} \equiv 1 \mod 5$. Il résulte par produit que $\boxed{4^{2k+1} \equiv 4 \mod 5}$.
   Conclusion : $4^n - 1$ est divisible par 5 **si et seulement si** n est pair. (**équivalence**)
5. Diviseurs premiers de $4^{28} - 1$: la question 2 a déjà donné le nombre 29 ; la question 3 a donné le diviseur premier 17 ; la question 4 a donné le diviseur 5.
   D'autre part, $4 \equiv 1 \mod 3$ entraîne $4^n \equiv 1 \mod 3$ ou encore $4^n - 1$ est divisible par 3 qui est premier. Il y a également 5, 43.

Partie B. Divisibilité par un nombre premier

1. $4 = 2^2$; si p est premier différent de 2, il est premier avec 4, donc d'après le petit théorème de Fermat $4^{p-1} - 1 \equiv 0 \mod p$ ou $\boxed{4^{p-1} \equiv 1 \mod p}$.

   Le premier premier différent de 2 est 3, donc $\boxed{n = p - 1 \geqslant 1}$.
2. (a) On a donc : $4^n \equiv 1 \mod p$, $4^b \equiv 1 \mod p$ et $n = bq + r$ avec $r < b$. On déduit de la seconde congruence que $4^{bq} \equiv 1 \mod p$ et par quotient avec $4^{bq+r} \equiv 1 \mod p$ que $4^r \equiv 1 \mod p$.
   Or b étant le plus petit naturel vérifiant $4^b \equiv 1 \mod p$, il en résulte que $4^r = 1$ ou encore $\boxed{r = 0}$.

   (b) On vient démontrer dans la question précédente que si $4^n \equiv 1 \mod p$, alors n est multiple de b, b étant le plus naturel positif tel que $4^b \equiv 1 \mod p$.

   Réciproquement : si $n = kb$, de $4^b \equiv 1 \mod p$, on déduit que $\left(4^b\right)^k \equiv 1^k \mod p$ soit $4^n \equiv 1 \mod p$. L'équivalence est donc démontrée.

   (c) D'après la question B. 1 $4^{p-1} \equiv 1 \mod p$ et soit b le plus petit entier tel que $4^b \equiv 1 \mod p$. D'après la question 2. b. il en résulte que $p - 1$ est multiple de b ou encore b (non nul) divise $p - 1$.