Exercice 1 : arithmétique (12.5 points)

1. Soit $n \in \mathcal{E}$.
   Supposons n pair.
   Alors 2 divise n, et n divise $2^n + 1$, donc 2 divise $2^n + 1$ (*par transitivité*).
   Comme $n \geq 1$, 2 divise 2^n.
   Par conséquent, 2 divise $(2^n + 1) - 2^n = 1$. **Contradiction**.

   Ainsi, tout élément de $\mathcal{E}$ est impair **(1.25 pt)**

2. Soit $P(k)$: « 3^k appartient à $\mathcal{E}$ »
   1 divise $2^1 + 1$, donc $P(0)$ est vraie.
   3 divise $2^3 + 1$, donc $P(1)$ est vraie.
   Supposons $P(k)$ vraie pour un entier $k \geq 1$.
   $2^{3^{k+1}} + 1 = 2^{3^k \times 3} + 1 = (2^{3^k})^3 + 1 = (2^{3^k} + 1)(4^{3^k} - 2^{3^k} + 1)$
   D'après $P(k)$, $2^{3^k} + 1$ est un multiple de 3^k.
   Il reste à montrer que $4^{3^k} - 2^{3^k} + 1$ est un multiple de 3.
   Or d'après $P(k)$, $2^{3^k} + 1$ est un multiple de 3^k, donc est un multiple de 3.
   D'où : $2^{3^k} \equiv -1 \ [3]$.
   Et $4^{3^k} \equiv 1 \ [3]$.
   Par conséquent, $4^{3^k} - 2^{3^k} + 1 \equiv 0 \ [3]$.
   On peut ainsi déduire que $2^{3^{k+1}} + 1$ est un multiple de 3^{k+1} : $P(k+1)$ est vraie.

   On a ainsi montré que pour tout $k \in \mathbb{N}$, le nombre 3^k appartient à $\mathcal{E}$ **(2 pts)**

3. (a) Comme n est impair, p est impair, et donc $p - 1$ est pair.
   On peut écrire : $p - 1 = 2q$ avec $q \in \mathbb{N}^*$.

   Comme p est le plus petit diviseur premier de n, le seul diviseur de n de l'ensemble $[\![1, p-1]\!]$ est le nombre 1.
   Et q est un nombre entier de l'ensemble $[\![1, p-1]\!]$.
   Par conséquent, n et q n'ont pas de diviseur commun autre que 1.
   n et q sont donc premiers entre eux : $n \wedge q = 1$.

   On a ainsi : $(2n) \wedge (p-1) = (2n) \wedge (2q) = 2 \times (n \wedge q) = 2$ **(2 pts)**

   (b) p est un nombre premier, et 2 est premier avec p.
   Donc d'après le petit théorème de Fermat, $2^{p-1} \equiv 1 \ [p]$

   Ainsi, $p - 1$ appartient à A **(0.75 pt)**

   p divise n, et n divise $2^n + 1$, donc p divise $2^n + 1$.
   Par conséquent, $2^n \equiv -1 \ [p]$
   D'où $(2^n)^2 \equiv 1 \ [p]$, ce qui donne : $2^{2n} \equiv 1 \ [p]$

   Ainsi, $2n$ appartient à A **(0.75 pt)**

   (c) A est une partie non vide de $\mathbb{N}$, donc A possède un plus petit élément a **(0.25 pt)**

   (d) Supposons que k appartienne à A : $2^k \equiv 1 \ [p]$

   Effectuons la division euclidienne de k par a : $k = aq + r$ avec $0 \leq r < a$.
   On a alors : $2^k = (2^a)^q \times 2^r$.
   Comme a est un élément de A, on a : $2^a \equiv 1 \ [p]$
   Par hypothèse, $2^k \equiv 1 \ [p]$
   $(2^a)^q \times 2^r \equiv 1 \ [p]$
   $2^r \equiv 1 \ [p]$

   Si r était non nul, alors r serait un élément de A, ce qui est exclu car $r < a$.
   On en déduit que $r = 0$. Donc $k = aq$ est un multiple de a.

   On a montré que si $k \in A$, alors k est un multiple de a **(2 pts)**

(e) a divise tout élément de A, donc a divise les nombres $2n$ et $p-1$.
a divise donc leur PGCD : a divise 2 (en utilisant le résultat de la question a).
Comme $1 \notin A$, $\boxed{\text{on en déduit que } a = 2}$ **(0.75 pt)**

p divise $2^a - 1$, donc p divise 3.
$\boxed{\text{Par conséquent, } p = 3}$ **(0.25 pt)**

4. (a) Supposons que $n \in \mathcal{E}$ (ie n divise $2^n + 1$).
On peut écrire : $2^n + 1 = nq$ avec $q \in \mathbb{N}^*$.
Comme $2^n + 1$ est impair, q est impair.
Par conséquent, $(-1)^q = -1$.

D'où : $2^{2^n+1} + 1 = 2^{nq} + 1 = (2^n)^q - (-1)^q = \Big(2^n + 1\Big) \displaystyle\sum_{k=0}^{q-1} (-1)^k (2^n)^{q-1-k}$

On a ici utilisé l'identité remarquable $a^q - b^q = (a-b) \displaystyle\sum_{k=0}^{q-1} a^{q-k-1} b^k$

Ce qui prouve que $2^{2^n+1} + 1$ est un multiple de $2^n + 1$.
$\boxed{\text{On a montré que si } n \in \mathcal{E}, \text{ alors } 2^n + 1 \in \mathcal{E}}$ **(2 pts)**

(b) 9 appartient à $\mathcal{E}$, donc d'après ce qui précède, le nombre $2^9 + 1 = 513$ appartient à $\mathcal{E}$ (et ce n'est pas une puissance de 3). **(0.5 pt)**

Exercice 2

1. (a) La relation $ab = n^2$ donne : $ukb = u^2v^2$ puis $kb = uv^2$ (après simplification par u qui est non nul).

k et v sont les quotients respectifs de a et n par leur PGCD.
D'après la caractérisation du PGCD, k et v sont premiers entre eux.
k est donc premier avec v^2 et divise le produit uv^2, par conséquent k divise u d'après le théorème de Gauss.

u est un diviseur de a, et a est premier avec b, donc u est premier avec b (tout diviseur commun de u et b est un diviseur commun de a et b).
De plus, u divise le produit kb.
Donc u divise k d'après le théorème de Gauss.

(b) u et k sont deux entiers positifs associés, donc $u = k$.
Ce qui donne : $a = u^2$.

De la relation $ab = n^2$, on obtient : $u^2 b = u^2 v^2$, puis $b = v^2$.

Soit $d = u \wedge v$.
d divise u et v, donc d divise $a = u^2$ et $b = v^2$.
Par conséquent, d divise $a \wedge b = 1$, donc $d = 1$. Ainsi, $u \wedge v = 1$.

2. (a) Notons $d = x \wedge z$.
d divise x et z, donc d divise la combinaison linéaire $z^2 - x^2 = y^2$.
d divise ainsi x et y^2.
Comme x et y sont premiers entre eux, x et y^2 sont également premiers entre eux.
Par conséquent, $d = 1$.
$\boxed{\text{Ainsi, } x \wedge z = 1}$

(b) Soient a et b deux entiers impairs. On note $a = 2k + 1$ et $b = 2k' + 1$ où $k \in \mathbb{Z}$ et $k' \in \mathbb{Z}$.
$a^2 + b^2 = 4k^2 + 4k + 1 + 4k'^2 + 4k' + 1$, $\boxed{\text{d'où } a^2 + b^2 \equiv 2 \ [4]}$

(c) x et y sont premiers entre eux, donc x et y ne peuvent pas être tous les deux pairs.
Si x et y étaient tous les deux impairs, alors on aurait : $z^2 \equiv 2 \ [4]$
Ce qui est impossible, car le carré d'un entier est congru à 0 ou à 1 modulo 4 (suivant qu'il est pair ou impair).

$\boxed{\text{Ainsi, } x \text{ et } y \text{ sont de parités différentes}}$

Raisonnons modulo 2 pour déduire la parité de z.

Supposons par exemple que x soit pair et y soit impair.
Alors $x \equiv 0\ [2]$ et $y \equiv 1\ [2]$, puis $x^2 + y^2 \equiv 1\ [2]$, c'est-à-dire $z^2 \equiv 1\ [2]$
Ce qui entraîne que $z \equiv 1\ [2]$ (car $z \equiv 0\ [2]$ n'est pas compatible avec $z^2 \equiv 1\ [2]$)

$\boxed{z \text{ est impair}}$

(d) y et z sont deux entiers impairs, donc $z - y$ et $z + y$ sont pairs, ce qui justifie que a **et** b **sont des entiers.**

Notons $d = a \wedge b$.
d divise a et b, donc d divise $z = a + b$ et $y = a - b$.
Puis d divise $z^2 - y^2 = x^2$.
Comme y et x^2 sont premiers entre eux, on en déduit que $d = 1$.

Enfin, $ab = \dfrac{z+y}{2} \times \dfrac{z-y}{2} = \dfrac{z^2 - y^2}{4} = \dfrac{x^2}{4} = n^2$

(e) D'après le résultat préliminaire, il existe deux entiers naturels u et v premiers entre eux tels que $a = u^2$ et $b = v^2$.
On a alors : $y = a - b = u^2 - v^2$, $z = a + b = u^2 + v^2$ et $x = 2n = 2\sqrt{ab} = 2uv$
Il reste à justifier que u et v sont de parités différentes.
Si u et v étaient tous deux impairs, alors y serait pair (différence de deux nombres impairs), ce qui est exclu.
Si u et v étaient tous deux pairs, alors y serait pair également.
Par conséquent, u et v sont nécessairement de parités différentes.

3. (a) $x^2 + y^2 = 4u^2v^2 + (u^2 - v^2)^2 = u^4 + 2u^2v^2 + v^4 = (u^2 + v^2)^2 = z^2$.
Donc (x, y, z) est un triplet pythagoricien.

(b) Notons $d = y \wedge z$.
d divise $2u^2 = z + y$ et d divise $2v^2 = z - y$.
Or z est impair (somme d'un nombre pair et d'un nombre impair), z n'est pas divisible par 2,
donc d n'est pas divisible par 2.
2 et d sont donc premiers entre eux.
Le théorème de Gauss permet alors de déduire que d divise u^2 et v^2.
Comme u^2 et v^2 sont premiers entre eux, on obtient que $d = 1$.

Le même raisonnement que celui tenu à la question 2a permet d'établir que $x \wedge y = 1$.

4. IL suffit de choisir un couple (u, v) d'entiers premiers entre eux et de parités différentes avec $u > v$, puis d'appliquer les formules données à la question 3 pour obtenir un triplet pythagoricien primitif.
Voici 10 exemples possibles :

u	v	$x = 2uv$	$y = u^2 - v^2$	$z = u^2 + v^2$
4	1	8	15	17
6	1	12	35	37
8	1	16	63	65
10	1	20	99	101
3	2	12	5	13

u	v	$x = 2uv$	$y = u^2 - v^2$	$z = u^2 + v^2$
5	2	20	21	29
7	2	28	45	53
4	3	24	7	25
5	4	40	9	41
6	5	60	11	61