Correction des exercices sur les nombres premiers

Exercice 1
Partie A

1. On a $a = b + (a-b) \equiv b\ [a-b]$ donc, par théorème, $\boxed{a^n \equiv b^n\ [a-b]}$.

2. On applique le résultat de la question **1.** avec $b = 1$. Ceci est possible car $a \geqslant 2$ donc $a > 1$. Il vient alors $a^n \equiv 1^n\ [a-1]$ i.e. $a^n \equiv 1\ [a-1]$ et donc, par définition, $\boxed{a-b \text{ divise } a^n - 1}$.

3. On applique le résultat de la question **1.** avec $b = -1$. Ceci est possible car $a \geqslant 2$ donc $a > -1$. Il vient alors $a^n \equiv (-1)^n\ [a-(-1)]$. Or, n est impair donc $(-1)^n = -1$ et donc $a^n \equiv -1\ [a+1]$. Par définition, $a+b$ divise $a^n - (-1)$ i.e. $\boxed{a+b \text{ divise } a^n + 1}$.

Partie B

1. Supposons que $a^n - 1$ est premier. Alors, les seuls diviseurs positifs de $a^n - 1$ sont 1 et $a^n - 1$. Or, d'après la question **2.** de la **partie A**, $a-1$ est un diviseur de $a^n - 1$. De plus, comme $n \geqslant 2$ et $a > 0$, $a^n > a$ donc $a^n - 1 > a - 1$. Il s'ensuit que $a - 1 = 2$ i.e. $\boxed{a = 2}$.

2. On obtient le tableau suivant :

k	2	3	4	5	6	7	8	9	10
M_k	3	7	15	31	63	127	255	511	1023

3. D'après la liste donnée dans l'énoncé, les nombres $M_2 = 3$, $M_3 = 7$ et $M_5 = 31$ sont premiers. De plus, on vérifie que $M_7 = 127$ n'a pas de diviseur premier inférieur à $E(\sqrt{127}) = 11$ donc il est également premier. Au vu du tableau, on peut donc conjecturer que (P) est vraie.

4. a. Le nombre $M_{11} = 2047$ est divisible par 23 car $2047 = 23 \times 89$ donc il n'est pas premier.

b. Comme 11 est premier mais M_{11} est composé, l'implication (P) est fausse.

5. a. L'implication (Q) est « pour tout entier $n \geqslant 2$, si M_n est premier alors n est premier ». La contraposée de (Q) est « pour tout entier $n \geqslant 2$, si n n'est pas premier alors M_n n'est pas premier ».

b. Comme $p \geqslant 1$, $2^p \geqslant 2$. On peut donc appliquer le résultat de la question **2.** de la **partie A** en prenant $a = 2^p$ et $n = q$. Il vient que $2^p - 1$ divise $(2^p)^q - 1 = 2^{pq} - 1$ i.e. $\boxed{M_p \text{ divise } M_{pq}}$.

c. Soit $n \geqslant 2$ un entier qui n'est pas premier. Alors, n admet deux diviseurs stricts $p \geqslant 2$ et $q \geqslant 2$ tels que $n = pq$. On déduit de la question précédente que M_p divise M_n et, comme $2 \leqslant p \leqslant n-1$, $M_p \notin \{1, M_n\}$. Ainsi, on peut conclure que $\boxed{M_n \text{ n'est pas premier}}$.

d. La question précédente montre que la contraposée de (Q) est vraie et donc on conclut que $\boxed{\text{(Q) est également vraie}}$.

Partie C

1. a. Supposons que a est impair. Alors, $a \geqslant 3$ donc $a^n + 1 \geqslant 4$. De plus, comme a est impair, a^n aussi donc $a^n + 1$ est pair. Ainsi, $a^n + 1$ est un nombre pair au moins égal à 4 : il n'est donc pas premier.

b. Par hypothèse, il existe un entier $q \geqslant 1$ tel que $n = pq$. Comme $a \geqslant 2$, $a^q \geqslant 2$. Comme p est impair, d'après la question **3.** de la **partie A**, $a^q + 1$ divise $(a^q)^p + 1 = a^n + 1$. De plus, comme $a^q > 0$ et $q \geqslant 3$, $1 < a^q + 1 < a^n + 1$. Ainsi, $\boxed{a^n + 1 \text{ n'est pas premier}}$.

2. Si on considère $a = 6$ et $n = 2$ alors $a^n + 1 = 37$ est premier et $a = 2 \times 3$ admet un diviseur premier impair.

3. Pour tout entier $n \geqslant 2$, on pose $F_n = 2^{2^n} + 1$.

a. Soit un entier $n \geqslant 2$. Alors,

$$F_{n+1} - 2 = 2^{2^{n+1}} + 1 - 2 = 2^{2^n \times 2} - 1 = \left(2^{2^n}\right)^2 - 1^2 = \left(2^{2^n} + 1\right)\left(2^{2^n} - 1\right)$$

i.e. $\boxed{F_{n+1} - 2 = F_n(F_n - 2)}$.

b. Soit un entier $n \geqslant 2$. Alors, 2^{2^n} est pair donc F_n est impair. Supposons que F_n soit la somme de deux nombres premiers p et q avec $p \leqslant q$. Comme la somme de deux nombres de même parité est paire, p et q sont de parité contraire. Il s'ensuit que $p = 2$ et $q = F_n - p = F_n - 2$.
Si $n = 2$ alors $q = 2^{2^2} + 1 - 2 = 15$ qui n'est pas premier. C'est absurde.
Si $n > 2$ alors, d'après la question **a.**, $q = F_{n-1}(F_{n-1} - 2)$ donc F_{n-1} et $F_{n-1} - 2$ divise q. Comme q est premier et $0 < F_{n-1} - 2 < F_{n-1}$, il s'ensuit que $F_{n-1} - 2 = 1$ i.e. $F_{n-1} = 3$. C'est absurde car $n \geqslant 3$ donc $F_{n-1} \geqslant 2^{2^{3-1}} - 1 = 15$.
Ainsi, pour tout entier $n \geqslant 2$, $\boxed{F_n \text{ n'est pas la somme de deux nombres premiers}}$.

Exercice 2

1. Les trois plus petits éléments de $\mathcal{A}_1$ qui sont des nombres premiers sont 5, 13 et 17 et les trois plus petits éléments de $\mathcal{A}_3$ qui sont des nombres premiers sont 3, 7 et 11.

2. Soit p un nombre premier différent de 2 et r le reste de p modulo 4. Alors, il existe $k \in \mathbb{N}$ tel que $p = 4k + r$. Or, p est impair donc $r = p - 4k$ est impair. Ainsi, comme $r \in \{0, 1, 2, 3\}$, $r = 1$ ou $r = 3$. Si $r = 1$ alors $p = 4k + 1$ donc $p \in \mathcal{A}_1$ et si $r = 3$ alors $p = 4k + 3$ donc $p \in \mathcal{A}_3$. On a donc bien montré que tout nombre premier $p \neq 2$ appartient à $\mathcal{A}_1$ ou à $\mathcal{A}_3$.

3. Pour tout $m \in \mathbb{N}^*$, le nombre $a_m = 12m + 3 = 4 \times (3m) + 3$ appartient à $\mathcal{A}_3$ puisque $3m \in \mathbb{N}$. De plus, $a_m = 3(4m + 1)$ est divisible par 3 et $a_m > 3$ car $m > 0$. Dès lors, a_m n'est pas premier. De plus, la suite (a_m) est strictement croissante donc contient une infinité de valeurs différentes. Ainsi, (a_m) fournit une infinité d'éléments de $\mathcal{A}_3$ qui ne sont pas premiers.

4. **a.** Supposons qu'un entier N s'écrive $N = q_1 q_2 \cdots q_n$ où les nombres q_i sont des nombres premiers appartenant à $\mathcal{A}_1$. Alors, pour tout entier i compris entre 1 et n, $q_i \equiv 1$ [4] donc $q_1 q_2 \cdots q_n \equiv 1^n$ [4] i.e. $N \equiv 1$ [4]. Il existe donc $k \in \mathbb{N}$ tel que $N = 4k + 1$ donc $N \in \mathcal{A}_1$.

b. Remarquons que $N = 4p_1 p_2 \cdots p_n - 1$ est impair donc tous ses diviseurs premiers sont impairs. Ils sont donc soit dans $\mathcal{A}_1$ soit dans $\mathcal{A}_3$ d'après la question **2.**. Supposons que tous les diviseurs premiers de N soient dans $\mathcal{A}_1$. Alors, d'après la question précédente, $N \in \mathcal{A}_1$ i.e. $N \equiv 1$ [4]. Or, $N \equiv -1$ [4] donc $1 \equiv -1$ [4] i.e. $2 \equiv 0$ [4] ce qui signifie que 4 divise 2. Ceci est évidemment faux donc N possède au moins un diviseur premier $p \in \mathcal{A}_3$. Mais alors p est l'un des nombres p_1, p_2, ..., p_n donc p divise $p_1 p_2 \cdots p_n$. Ainsi, p divise N et p divise $p_1 p_2 \cdots p_n$ donc p divise $N - p_1 p_2 \cdots p_n = -1$ donc $p = 1$ car $p > 0$. C'est absurde car p est premier.
On conclut donc que l'ensemble $\mathcal{A}_3$ contient une infinité de nombres premiers.