Le but de l'exercice est d'étudier la primalité de l'entier $N = 2^{17} - 1$.
On admet la proposition suivante : si p est un nombre premier impair, alors $2^{p-1} \equiv 1 \pmod{p}$

1. *a.* Contrôler la véracité de cette proposition pour $p = 5$ et $p = 7$

b. Soit k un entier et n un multiple de k, montrer que si $2^k \equiv 1 \pmod{p}$ alors $2^n \equiv 1 \pmod{p}$

Soit p un facteur premier éventuel de N.

2. *a.* Montrer que p est impair et que $2^{17} \equiv 1 \pmod{p}$

b. Soit b le plus petit entier naturel non nul tel que $2^b \equiv 1 \pmod{p}$, soit n un entier naturel tel que $2^n \equiv 1 \pmod{p}$. Montrer que n est un multiple de b. (utiliser la division euclidienne de n par b)

c. En déduire que b divise 17 puis que $b = 17$

d. En déduire que $p - 1$ est un multiple de 17

e. Expliquer pourquoi il suffit de chercher p sous la forme $34m + 1$ ou m est un entier naturel

CORRECTION

1. *a.* $2^{5-1} = 16$ or $16 = 3 \times 5 + 1$ donc $2^{5-1} \equiv 1 \pmod{5}$
$2^{7-1} = 64$ or $64 = 9 \times 7 + 1$ donc $2^{7-1} \equiv 1 \pmod{7}$
La proposition est vérifiée pour $p = 5$ et $p = 7$

b. Soit k un entier et n un multiple de k donc il existe un entier m tel que $n = mk$
si $2^k \equiv 1 \pmod{p}$ alors $(2^k)^m \equiv 1^m \pmod{p}$ soit $2^{mk} \equiv 1 \pmod{p}$ donc $2^n \equiv 1 \pmod{p}$

2. *a.* Si p est pair, p étant un nombre premier, $p = 2$ or $N = 2^{17} - 1$ donc N est impair donc 2 ne divise pas N, p est impair
p un facteur premier éventuel de N donc $N \equiv 0 \pmod{p}$ soit $2^{17} - 1 \equiv 0 \pmod{p}$ donc $2^{17} \equiv 1 \pmod{p}$

b. Effectuons la division euclidienne de n par b, il existe deux entiers q et r tels que $n = bq + r$ et $0 \leq r < b$
$2^n = 2^{bq} \times 2^r$ or $2^b \equiv 1 \pmod{p}$ donc $2^{bq} \equiv 1 \pmod{p}$ donc $2^n \equiv 2^r \pmod{r}$
$2^n \equiv 1 \pmod{p}$ donc $2^r \equiv 1 \pmod{r}$

Deux cas se présentent pour r : soit $0 < r < b$ soit $r = 0$
Montrons que le cas $0 < r < b$ est impossible
b est le plus petit entier naturel non nul tel que $2^b \equiv 1 \pmod{p}$, et $2^r \equiv 1 \pmod{r}$ donc si $0 < r < b$ alors r serait le plus petit entier tel que $2^r \equiv 1 \pmod{p}$ et non b donc cette hypothèse est erronée, $r = 0$ donc $n = bq$, n est un multiple de b.

c. b le plus petit entier naturel non nul tel que $2^b \equiv 1 \pmod{p}$, $2^{17} \equiv 1 \pmod{p}$ donc d'après la question précédente, 17 est un multiple de b donc b divise 17 donc $b = 1$ ou $b = 17$.
$2^1 = 2$ or p est un nombre premier impair donc $p \geq 3$, $2 - 1 = 1$ et p ne divise pas 1 donc 2 n'est pas congru à 1 modulo p donc $b \neq 1$ donc $b = 17$

d. $2^{p-1} \equiv 1 \pmod{p}$ or d'après la question **2. *b.***, $p - 1$ est un multiple de b soit $p - 1$ est un multiple de 17

e. $p - 1$ est un multiple de 17 donc il existe un entier k tel que $p - 1 = 17k$
p est un nombre premier impair donc $p - 1$ est pair donc 2 divise $17k$, 2 et 17 sont premiers entre eux donc d'après le théorème de Gauss, 2 divise k, il existe un entier m tel que $k = 2m$
En remplaçant : $p - 1 = 17 \times 2m$ soit $p = 34m + 1$