CHAPITRE VII : ARITHMÉTIQUE

Correction

On a $a^p - 1 = (a-1)(a^{p-1} + a^{p-2} + ... + 1)$ donc si $a > 2$, on a $a - 1 \geqslant 2$ qui se retrouve être un diviseur non trivial de $a^p - 1$. Par conséquent, $a^p - 1$ n'est pas premier. Par contraposée, si $a^p - 1$ est premier alors $a = 2$.
Par ailleurs, si p n'est pas premier alors on peut décomposer p sous la forme $p = bd$ avec $b \geqslant 2$ et $d \geqslant 2$. Il s'ensuit

$$a^p - 1 = a^{bd} - 1 = (a^b)^d - 1 = (a^b - 1)\sum_{k=0}^{d-1} a^{bk}.$$

Comme $a \geqslant 2$ et $b \geqslant 2$, on a $a^b > 2$ donc $a^b - 2$ est un diviseur non trivial de $a^p - 1$ et $a^p - 1$ n'est pas premier. Par contraposée, si $a^p - 1$ est premier alors p est premier.
Finalement, si $a^p - 1$ est premier alors $a = 2$ et p est premier.