Exercice n° 12

Montrons que : ($a^p - 1$ est premier) $\Longrightarrow$ ($a = 2$ et p est premier)

- Supposons que $a \neq 2$;

Comme $3^2 - 1 = 9 - 1 = 8$ et que 8 n'est pas premier

alors si $a \neq 2$, alors $a^p - 1$ n'est pas premier

- Supposons que p n'est pas premier ;

alors il existe n et m appartenant à $\mathbb{N}$ tels que

$p = nm$ avec $1 < n < p$ et $1 < m < p$.

Donc $a^p - 1 = a^{nm} - 1 = (a^n)^m - 1 = (a^n)^m - 1^m$;

d'où $a^p - 1 = (a^n - 1)\left[1 + a^n + (a^n)^2 + \cdots + (a^n)^{m-1}\right]$

or $\begin{cases} a \geq 2 \text{ et } n > 1 \Longrightarrow a^n - 1 \geq 3 \\ m > 1 \Longrightarrow a^n - 1 < (a^n)^m - 1 \end{cases}$

donc $a^n - 1$ est un diviseur propre de $a^p - 1$;

ainsi $a^p - 1$ n'est pas un nombre premier.

Comme $[a \neq 2$ ou p n'est pas premier$] \Longrightarrow [a^p - 1$ n'est pas premier$]$

alors $[a^p - 1$ est premier$] \Longrightarrow [a = 2$ et p est premier$]$.