

DEVOIR MAISON 12

► Problème : théorème LTE (Lifting the exponent)

Soit p un nombre premier, et soient x, y deux entiers relatifs, premiers à p avec $|x| \neq |y|$.

1. On suppose que p divise $x - y$. Montrer que pour tout $n \in \mathbf{N}^*$ premier à p , $v_p(x^n - y^n) = v_p(x - y)$.
2. Dans cette question, on suppose que $p = 2$, et que $4 \mid x - y$.
 - a. Montrer que $v_2(x^2 - y^2) = v_2(x - y) + 1$.
 - b. Prouver par récurrence que pour tout $n \in \mathbf{N}^*$, $v_2(x^n - y^n) = v_2(x - y) + v_2(n)$.
3. On suppose à présent que p est impair, et que $p \mid x - y$.
 - a. Prouver que pour tout $k \in \llbracket 1, p-1 \rrbracket$, $x^k \equiv y^k + k(x - y)y^{k-1} \pmod{p^2}$.
 - b. En déduire que $\sum_{k=0}^{p-1} x^k y^{p-1-k} \equiv py^{p-1} \pmod{p^2}$, puis que $v_p(x^p - y^p) = v_p(x - y) + 1$.
 - c. Prouver alors que pour tout $n \in \mathbf{N}^*$, $v_p(x^n - y^n) = v_p(x - y) + v_p(n)$.
4. Application : soit $k \in \mathbf{N}^*$ fixé. Trouver tous les $n \in \mathbf{N}$ tels que $3^k \mid 2^n - 1$.
Indication : distinguer le cas n pair du cas n impair.