LIFTING THE EXPONENT (INDICATIONS/ALERTES)

Remarque préliminaire : L'hypothèse : $|x| \neq |y|$ sert juste à garantir que : $x^n \neq y^n$ pour tout $n \in \mathbb{N}^*$, et donc que la valuation p-adique $v_p\big(x^n - y^n\big)$ est bien définie.

1)

2)

3) a) Formule du binôme !

b) Simplifier la somme grâce à **a)**, calculer $\displaystyle\sum_{k=1}^{p-1} k$ et observer que $\dfrac{p-1}{2}$ est entier.

4) Récurrence forte ! Pour en comprendre le principe, prenons l'exemple d'un entier n de la forme : $n = p^2 m$ avec p impair et $m \in \mathbb{N}^*$ premier à p. Aussitôt :

$$v_p\big(x^n - y^n\big) = v_p\big(x^{p^2 m} - y^{p^2 m}\big) \overset{\textbf{3)b)}}{=} v_p\big(x^{pm} - y^{pm}\big) + 1 \overset{\textbf{3)b)}}{=} v_p\big(x^m - y^m\big) + 2 \overset{\textbf{1)}}{=} v_p(x-y) + 2.$$

À charge pour vous maintenant de rédiger soigneusement cette récurrence.

5) Traduire le problème en termes de valuations 2-adiques et appliquer **1)**.

6) Montrer d'abord que les entiers $x-1$ et $x+1$ sont des puissances de p. Après discussion : $p = 2$ et $x = n = 3$.

7)

8) a) Par imparité de n, $p+1$ divise $p^n + 1$.

b) Par exemple : $2^{q'} \equiv 1 \big[2^{q'} - 1\big]$. Si on note r le reste de la division euclidienne de q par q', le reste de la division euclidienne de $2^q - 1$ par $2^{q'} - 1$ vaut $2^r - 1$.

c)

9) a)

b)

c) Appliquer théorème LTE à l'entier $x^q - 1$ après en avoir soigneusement vérifié les hypothèses.

d) Montrer grâce à **c)** que : $p^n > p^{(n-1)q}$.

10)