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, $v_p\left(x^n - y^n\right) = v_p(x - y)$.
2. Dans cette question, on suppose que $p = 2$, et que $4 \mid x - y$.
   a. Montrer que $v_2\left(x^2 - y^2\right) = v_2(x - y) + 1$.
   b. Prouver par récurrence que pour tout $n \in \mathbf{N}^*$, $v_2\left(x^n - y^n\right) = v_2(x - y) + v_2(n)$.
3. On suppose à présent que p est impair, et que $p \mid x - y$.
   a. Prouver que pour tout $k \in [\![1, p-1]\!]$, $x^k \equiv y^k + k(x-y)y^{k-1} \ [p^2]$.
   b. En déduire que $\displaystyle\sum_{k=0}^{p-1} x^k y^{p-1-k} \equiv py^{p-1} \ [p^2]$, puis que $v_p\left(x^p - y^p\right) = v_p(x - y) + 1$.
   c. Prouver alors que pour tout $n \in \mathbf{N}^*$, $v_p\left(x^n - y^n\right) = v_p(x - y) + v_p(n)$.
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.

CORRECTION DU DEVOIR MAISON 12

▸ Problème : théorème LTE

1. Il s'agit d'utiliser la troisième identité remarquable généralisée : $x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k}$.

Il vient alors

$$v_p\left(x^n - y^n\right) = v_p(x-y) + v_p\left(\sum_{k=0}^{n-1} x^k y^{n-1-k}\right).$$

Il s'agit donc de prouver que $v_p\left(\sum_{k=0}^{n-1} x^k y^{n-1-k}\right) = 0$.

Mais modulo p, on $x - y \equiv 0 \ [p]$, et donc $x \equiv y \ [p]$.

Donc pour tout $k \in [\![0, n-1]\!]$, $x^k y^{n-1-k} \equiv x^k x^{n-1-k} \equiv x^{n-1} \ [p]$.

Et donc $\sum_{k=0}^{n-1} x^k y^{n-1-k} \equiv n x^{n-1} \ [p]$.

Mais n et x étant premiers à p, nx^{n-1} est aussi premier à p.

Et donc nx^{n-1} n'est pas divisible par p, si bien que $\sum_{k=0}^{n-1} x^k y^{n-1-k}$ n'est pas non plus[1] divisible par p, et donc $v_p\left(\sum_{k=0}^{n-1} x^k y^{n-1-k}\right) = 0$.

On a donc bien $v_p(x^n - y^n) = v_p(x-y) + 0 = \boxed{v_p(x-y).}$

Rappel

$v_p(ab) = v_p(a) + v_p(b)$.

[1] Ils sont congrus modulo p, et

$$nx^{n-1} \not\equiv 0 \quad [p].$$

2.a. On a $x^2 - y^2 = (x-y)(x+y)$, et donc $v_2(x^2-y^2) = v_2(x-y) + v_2(x+y)$.

Or x et y sont premiers à 2, donc impairs.

On a donc $4 \mid x - y \Leftrightarrow x \equiv y \ [4]$.

Or, $x \equiv 1 \ [4]$ ou $y \equiv 3 \ [4]$.

Mais $1 \not\equiv -1 \ [4]$ et $y \not\equiv -3 \ [4]$, si bien que $x \not\equiv -y \ [4] \Leftrightarrow x + y \not\equiv 0 \ [4]$.

Et donc 4 ne divise pas $x + y$.

Mais $x + y$ est pair, donc $2 \mid x + y$, si bien que $v_2(x+y) = 1$.

Et donc $\boxed{v_2\left(x^2 - y^2\right) = v_2(x-y) + 1.}$

2.b. Prouvons le résultat par récurrence forte sur $n \in \mathbf{N}^*$.

Pour $n = 1$, c'est évident puisque $v_2(1) = 0$, et donc $v_2(x-y) = v_2(x-y) + v_2(1)$.

Soit $n \geqslant 2$ et supposons que pour tout $k \in [\![1, n-1]\!]$, $v_2\left(x^k - y^k\right) = v_2(x-y) + v_2(k)$.

▸ Si n est premier à 2, c'est-à-dire impair, alors d'après la question 1,

$$v_2\left(x^n - y^n\right) = v_2(x-y) = v_2(x-y) + v_2(n).$$

▸ Si n est pair, notons $n = 2^k q$, avec q impair (et donc $k = v_2(n) \geqslant 1$). Alors

$$\begin{aligned} v_2\left(x^n - y^n\right) &= v_2\left(\left(x^{2^{k-1}q}\right)^2 - \left(y^{2^{k-1}q}\right)^2\right) \\ &= v_2\left(\left(x^{2^{k-1}q}\right) - \left(x^{2^{k-1}q}\right)\right) + 1 \\ &= v_2(x-y) + v_2\left(2^{k-1}q\right) + 1 \\ &= v_2(x-y) + (k-1) + 1 = v_2(x-y) + k = v_2(x-y) + v_2(n). \end{aligned}$$

Détails

C'est la question 2.a, qui s'applique car $x \equiv y \ [4]$ et donc $x^{2^{k-1}q} \equiv y^{2^{k-1}q} \ [4]$ de sorte que

$$4 \mid x^{2^{k-1}q} - y^{2^{k-1}q}.$$

Hypothèse de récurrence car $2^{k-1}q < n$

Donc par le principe de récurrence, $\boxed{\text{pour tout } n \in \mathbf{N}^*,\ v_2\left(x^n - y^n\right) = v_2(x-y) + v_2(n).}$

3.a. Pour $k = 1$, on a $x^k = x = y + 1 \times (x-y)$, et donc l'égalité vaut évidemment modulo p^2.

Supposons donc que $k \in [\![2, p-1]\!]$.

Notons que $x = (y + (x-y))$, si bien que par le binôme de Newton,

$$x^k = (y + (x-y))^k = \sum_{j=0}^{k} \binom{k}{j} y^j (x-y)^{k-j} = \sum_{j=0}^{k-2} \binom{k}{j} y^j (x-y)^{k-j} + k y^{k-1}(x-y) + y^k.$$

Puisque $p \mid x-y$, pour $j \in [\![0, k-2]\!]$, $k-j \geqslant 2$, et donc $p^2 \mid (x-y)^{k-j}$, si bien que $\binom{k}{j} y^j (x-y)^{k-j} \equiv 0 \ [p^2]$.

Et donc $\boxed{x^k \equiv y^k + k(x-y)y^{k-1} \ [p^2].}$

3.b. On en déduit donc que $\displaystyle\sum_{k=0}^{p-1} x^k y^{p-1-k} \equiv y^{p-1} + \sum_{k=1}^{p-1} x^k y^{p-1-k} \ [p^2]$.

D'après la question précédente, on a donc

$$\sum_{k=0}^{p-1} x^k y^{p-1-k} \equiv y^{p-1} + \sum_{k=1}^{p-1} \left(y^{p-1} + k(x-y)y^{p-2} \right) \equiv py^{p-1} + (x-y)y^{p-2}\frac{p(p-1)}{2} \quad [p^2].$$

Mais puisque p est impair, $\dfrac{p-1}{2} \in \mathbf{N}$, et donc $p \mid \dfrac{p(p-1)}{2}$.

Puisque par ailleurs p divise $(x-y)$, $y^{p-2}(x-y)\dfrac{p(p-1)}{2} \equiv 0 \ [p^2]$.

Et donc on a bien $\displaystyle\sum_{k=0}^{p-1} x^k y^{p-1-k} \equiv py^{p-1} \ [p^2]$.

Toujours par la troisième identité remarquable, on a $x^p - y^p = (x-y)\displaystyle\sum_{k=0}^{p-1} x^k y^{p-1-k}$, et donc

$$v_p\left(x^p - y^p\right) = v_p(x-y) + v_p\left(\sum_{k=0}^{p-1} x^k y^{p-1-k}\right).$$

Mais $\displaystyle\sum_{k=0}^{p-1} x^k y^{p-1-k} \equiv py^{p-1} \ [p^2]$.

Puisque y est premier à p, y^{p-1} l'est aussi, si bien que py^{p-1} est divisible par p, et pas par p^2.

Puisqu'il existe $m \in \mathbf{Z}$ tel que $\displaystyle\sum_{k=0}^{p-1} x^k y^{p-1-k} = py^{p-1} + mp^2$, on en déduit que $\displaystyle\sum_{k=0}^{p-1} x^k y^{p-1-k}$ est divisible par p, et pas par p^2, autrement dit que sa valuation p-adique vaut 1.

Et donc on a bien $\boxed{v_p\left(x^p - y^p\right) = v_p(x-y) + 1.}$

> ⚠ **Attention !**
> Deux nombres congrus modulo p (ou p^2) n'ont pas nécessairement la même valuation p-adique. Par exemple, toutes les puissances de p sont congrues modulo p, et n'ont pas toutes la même valuation p-adique !

3.c. Il s'agit encore d'une récurrence forte comme à la question 2.b, sauf que cette fois il nous faudra distinguer non plus suivant la parité de n, mais suivant que n est ou non divisible par p.
Lorsqu'il est premier à p, alors on utilisera la question 1, et sinon l'hypothèse de récurrence et la question 3.b.

4. **Application.** Soit $n \in \mathbf{N}$.
▶ Supposons n impair. Soit alors $q \in \mathbf{N}$ tel que $n = 2q+1$.
Alors $2^n - 1 = 2 \times 4^q - 1$. Puisque $4 \equiv 1 \ [3]$, $2^n - 1 \equiv 2 - 1 \equiv 1 \ [3]$.
Donc 3 ne divise pas $2^n - 1$, et a fortiori 3^k ne divise pas $2^n - 1$.
▶ Supposons n pair. Soit $q \in \mathbf{N}^*$ tel que $n = 2q$.
Alors $2^n - 1 = 4^q - 1^q$.
Puisque $3 \mid 4 - 1$, par le résultat de la question 3,

$$v_3(2^n - 1) = v_3\left(4^q - 1^q\right) = v_3(4-1) + v_3(q) = 1 + v_3(q).$$

Mais $3^k \mid 2^n - 1 \Leftrightarrow v_3(3^k) \leqslant v_3\left(2^n - 1\right) \Leftrightarrow k \leqslant 1 + v_3(q) \Leftrightarrow v_3(q) \geqslant k - 1$.
Et donc $\boxed{3^k \text{ divise } 2^n - 1 \text{ si et seulement si } n \text{ est divisible par } 2 \times 3^{k-1}.}$