LIFTING THE EXPONENT

1 LE THÉORÈME LTE

Soient $p \in \mathbb{P}$ et $x, y \in \mathbb{Z}$ premiers à p avec : $|x| \neq |y|$.

1) On suppose $x-y$ divisible par p. Montrer que pour tout $n \in \mathbb{N}^*$ premier à p : $v_p\big(x^n - y^n\big) = v_p(x-y)$.

2) On suppose : $p = 2$ et $x-y$ divisible par 4. Montrer que : $v_2\big(x^2 - y^2\big) = v_2(x-y) + 1$.

3) On suppose p impair et $x-y$ divisible par p.

a) Montrer que pour tout $k \in [\![1, p-1]\!]$: $x^k \equiv y^k + k(x-y)y^{k-1} \left[p^2\right]$.

b) En déduire que : $\displaystyle\sum_{k=0}^{p-1} x^k y^{p-k-1} \equiv p y^{p-1} \left[p^2\right]$, puis que : $v_p\big(x^p - y^p\big) = v_p(x-y) + 1$.

4) Démontrer par récurrence sur n le théorème *LTE* (*lifting the exponent*) énoncé ci-dessous.

Théorème (LTE) Soient $p \in \mathbb{P}$, $n \in \mathbb{N}^*$ et $x, y \in \mathbb{Z}$ premiers à p avec : $|x| \neq |y|$. On suppose $x-y$ divisible par p si p est impair et par 4 si : $p = 2$.

Dans ces conditions : $v_p\big(x^n - y^n\big) = v_p(x-y) + v_p(n)$.

2 UN CAS PARTICULIER DU THÉORÈME DE MIHĂILESCU

Jusqu'en 2002, le *théorème de Mihăilescu* était appelé la *conjecture de Catalan*. Énoncée en 1844 par le mathématicien français Catalan, cette conjecture a résisté plus de 150 ans avant de céder à l'assaut final du mathématicien roumain Mihăilescu.

Théorème (Théorème de Mihăilescu) 8 et 9 sont les seules puissances entières consécutives…

… si on convient d'appeler *puissance entière* tout entier a^n dans lequel $a \geqslant 2$ et $n \geqslant 2$ sont des entiers.

S'il est tout à fait exclu qu'on démontre ce théorème TRÈS DIFFICILE, rien n'interdit qu'on en étudie un cas particulier. En vue de la suite, il est bon de remarquer que toute puissance au sens du théorème peut être écrite x^q pour certains entiers $x \geqslant 2$ et $q \in \mathbb{N}^*$ PREMIER.

5) Déterminer tous les nombres premiers q pour lesquels $3^q - 1$ est divisible par 2^q.

On se donne désormais une fois pour toutes $p, q \in \mathbb{P}$ et $x, n \geqslant 2$ deux entiers pour lesquels : $x^q - p^n = 1$.

6) Déterminer p, x et n sous l'hypothèse que : $q = 2$.

On suppose désormais : $q \geqslant 3$.

7) On suppose dans cette question que : $x = 2$ et que n est pair. Montrer que : $p^2 \equiv 1\ [8]$, puis dénicher une contradiction.

8) On suppose dans cette question que : $x = 2$ et que n est impair.

a) Montrer que pour un certain $q' \in \mathbb{P}$: $p = 2^{q'} - 1$. On pourra utiliser sans les redémontrer les résultats relatifs aux nombres de Mersenne étudiés en TD.

b) Calculer le reste de la division euclidienne de $2^q - 1$ par $2^{q'} - 1$ en fonction du reste de la division euclidienne de q par q'.

c) En déduire une contradiction.

9) On suppose dans cette question que : $x \geqslant 3$.

a) Montrer que pour un certain $m \in \mathbb{N}^*$: $x = p^m + 1$.

b) Montrer que : $p^m \geqslant 3$. On pourra raisonner par l'absurde et exploiter le résultat de la question **5)**.

c) Déduire du théorème LTE que : $x - 1 \geqslant p^{n-1}$.

d) Dénicher une contradiction.

10) Énoncer proprement le résultat de cette palpitante aventure.