Exercices sur le théorème LTE

Igor Kortchemski

- Rappels de cours -

Pour un entier $n \geq 1$ et un nombre premier p, on note $v_p(n)$ l'exposant de la plus grande puissance de p divisant n.

Théorème (Théorème LTE)**.**

Soit p un nombre premier **impair**. Soient a, b des nombres entiers relatifs et un entier $n \geq 1$. On suppose que p divise $a - b$ mais que $p \nmid a, p \nmid a$. Alors :

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

Lorsque n est impair, en changeant y en $-y$ on en déduit immédiatement le résultat suivant, également utile dans les applications.

Théorème (Théorème LTE bis)**.**

Soit p un nombre premier **impair**. Soient a, b des nombres entiers (non nécessairement positifs) et un entier $n \geq 1$ *impair* . On suppose que p divise $a + b$ mais que p ne divise ni a ni b. Alors :

$$v_p(a^n + b^n) = v_p(a + b) + v_p(n).$$

Rappelons que l'énoncé du théorème LTE est différent pour $p = 2$.

- Exercices -

Exercice 1 Trouver tous les nombres premiers p tels que $(p-1)^p + 1$ soit une puissance de p.

Exercice 2 (Compétition UNESCO 1995) Soient a, n deux entiers strictement positifs et p un nombre premier impair tel que $a^p \equiv 1 \pmod{p^n}$. Montrer que $a \equiv 1 \pmod{p^{n-1}}$.

Exercice 3 Soit p un nombre premier et $m, n \geq 1$ des entiers tels que $10^p + 11^p = m^n$. Montrer que $n = 1$.

Exercice 4 Soit k un entier strictement positif. Trouver tous les entiers strictement positifs n tels que 3^k divise $2^n - 1$.

Exercice 5 (Olympiades Balkaniques de Mathématiques 1993) Soit p un premier impair et m un entier tel qu'il existe des entiers $x, y > 1$ vérifiant $(x^p + y^p)/2 = ((x+y)/2)^m$. Montrer que $m = p$.

Exercice 6 Trouver toutes les solutions entières strictement positives de $x^{2009} + y^{2009} = 7^k$.

Exercice 7 (Olympiade Iran 2008) Soit a un entier strictement positif. On suppose que $4(a^n + 1)$ est le cube d'un entier pour tout entier positif n. Trouver a.

Exercice 8 Soient $a > b > 1$ deux entiers avec b impair. Soit n un entier strictement positif. On suppose que b^n divise $a^n - 1$. Montrer que $a^b > 3^n/n$.

- Solutions -

<u>*Solution de l'exercice 1*</u> On exclut d'abord le cas $p = 2$ qui convient bien, et on remarque qu'on peut alors appliquer le théorème LTE : $v_p((p-1)^p + 1) = v_p(p-1+1) + v_p(p) = 2$. Donc $(p-1)^p + 1 = p^2$, ou encore $(p-1)^{p-1} = p+1$. Donc $p-1$ divise $p+1$, et donc $p-1$ divise $p+1-(p-1) = 2$. Donc $p = 3$. On vérifie réciproquement que $p = 3$ convient aussi.

<u>*Solution de l'exercice 2*</u> Il est clair que a et p sont premiers entre eux. D'après le petit théorème de Fermat, $a^{p-1} \equiv 1 \pmod p$. Comme $a^p \equiv 1 \pmod p$, on en déduit que $a \equiv 1 \pmod p$. On peut donc utiliser le théorème LTE et on obtient $v_p(a-1) + 1 = v_p(a-1) + v_p(p) = v_p(a^p - 1)$. Par hypothèse, le dernier terme est supérieur ou égal à n. Il en découle que $v_p(a-1) \geq n-1$, ce qu'il fallait démontrer.

<u>*Solution de l'exercice 3*</u> D'après le théorème LTE, on a

$$nv_3(m) = v_3(m^n) = v_3(10^p + 11^p) = v_3(21) + v_3(p) = 1 + v_3(p)$$

Ainsi, si $p \neq 3$, on a $n = 1$. Si $p = 3$, on vérifie que $10^3 + 11^3 = 2331$ ne s'écrit pas sous la forme m^n avec $n \geq 2$.

<u>*Solution de l'exercice 4*</u> Soit $k \geq 1$ un entier tel que 3^k divise $2^n - 1$. En raisonnant modulo 3, on voit que n est pair. Écrivons donc $n = 2m$ avec $m > 0$. Alors 3^k divise $4^m - 1$. Comme 3 divise $4 - 1$, on peut appliquer le théorème LTE pour obtenir $v_3(4-1) + v_3(n) = v_3(4^n - 1) \geq k$. On en déduit que $v_3(n) \geq k-1$. Ainsi $2 \times 3^{k-1}$ divise n.

Réciproquement, le même raisonnement nous donne que 3^k divise $2^n - 1$ si $2 \times 3^{k-1}$ divise n.

<u>*Solution de l'exercice 5*</u> Par convexité de $x \mapsto x^p$, on a $(x^p + y^p)/2 \geq ((x+y)/2)^p$. Par hypothèse, il s'ensuit que $m \geq p$. Soit $d = \mathrm{PGCD}(x, y)$, $x = dX$, $y = dY$. L'équation se réécrit

$$2^{m-1}(X^p + Y^p) = d^{m-p}(X+Y)^m. \tag{1}$$

Premier cas : $X + Y$ n'est pas une puissance de 2. Soit alors q un diviseur premier impair de $X + Y$. Par le théorème LTE, $v_q(2^{m-1}(X^p + Y^p)) = v_q(X+Y) + v_q(p)$ et d'autre part $v_q(d^{m-p}(X+Y)^m) \geq mv_q(X+Y)$. Donc $v_q(X+Y) + v_q(p) \geq mv_q(X+Y)$. Ceci implique $m \leq 2$, et donc $m = p = 2$ car $m \geq p$, ce qui est exclu car p est impair.

Deuxième cas : $X + Y$ est une puissance de 2. Comme p est impair, $X + Y$ divise $X^p + Y^p$ et donc $v_2(X+Y) \leq v_2(X^p + Y^p)$. À présent, en prenant la valuation 2-adique dans l'égalité (1), on obtient $m - 1 + v_2(X+Y) \geq mv_2(X+Y)$. Ainsi $v_2(X+Y) \leq 1$, $X + Y \leq 2$, et donc $X = Y = 1$ et $m = p$.

<u>*Solution de l'exercice 6*</u> Déjà, $2009 = 7^2 \times 41$. Comme $x + y$ divise $x^{2009} + y^{2009}$, $x + y$ est une puissance de 7. On remarque aussi que si x et y sont multiples de 7, on peut tout diviser par 7 et juste changer l'exposant k ; on peut donc supposer que x et y sont premiers avec 7. Le théorème LTE nous garantit que $v_7(x^{2009} + y^{2009}) = v_7(x+y) + v_7(2009) = v_7(x+y) + 2$, donc $x^{2009} + y^{2009} = 49(x+y)$, donc

$$\frac{x^{2009} + y^{2009}}{x+y} = x^{2008} - x^{2007}y + x^{2006}y^2 - \cdots + y^{2008} = 49$$

Mais il est facile de vérifier que ce terme est beaucoup plus grand que 49. Par exemple, si on suppose $x > y$, on aura toujours $x^{2008} - x^{2007}y \geq 1$, $x^{2006}y^2 - x^{2005}y^3 \geq 1$ et ainsi de suite, de sorte que la somme totale sera au moins égale à 1004. Il n'y a donc pas de solutions.

<u>*Solution de l'exercice 7*</u> Il est clair que $a = 1$ convient. Montrons que c'est le seul. Supposons donc $a > 1$. Choisissons $n = 2m$ et remarquons que $a^2 + 1$ n'est pas une puissance de 2 car congru à 1 ou 2 modulo 4. Soit donc p un nombre premier impair tel que p divise $a^2 + 1$. Alors d'après le théorème LTE, $v_p(4(a^n + 1)) = v_p(a^2 + 1) + v_p(m)$. On choisit m de sorte que ce dernier terme soit congru à 1 modulo 3. Alors $4(a^n + 1)$ n'est pas un cube, contradiction.

<u>*Solution de l'exercice 8*</u> Il suffit de résoudre l'exercice pour b premier. En effet, si c'est le cas, si b n'est pas premier et q est un diviseur premier de b, alors $q^n \mid a^n - 1$, et donc $a^b > a^q > 3^n/n$.

Supposons donc $b = p$ premier (impair), et notons ω l'ordre de a modulo p. D'après le petit théorème de Fermat, $\omega \mid p-1$. Donc $\omega \leq p-1$.

Comme $p \mid a^n - 1$, $\omega \mid n$. Écrivons donc $n = \omega n_1$. D'après le théorème LTE, en notant v_p la valuation p-adique,

$$v_p(a^n - 1) = v_p((a^\omega)^{n_1} - 1) = v_p(a^\omega - 1) + v_p(n_1) \geq n$$

car $p^n \mid a^n - 1$.

Maintenant, comme $\omega \leq p-1$,

$$a^p > a^\omega - 1 \geq p^{v_p(a^\omega - 1)} \geq p^{n - v_p(n_1)} = \frac{p^n}{p^{v_p(n_1)}} \geq \frac{p^n}{n_1} = \frac{\omega p^n}{n} \geq \frac{3^n}{n}$$

car $p^n \geq 3^n$.