Exercices sur le théorème de Zsigmondy

Igor Kortchemski

- Rappels de cours -

On rappelle les résultats suivants :

Théorème (Théorème de Zsigmondy)**.**
Soient $a > b \geq 1$ des entiers strictement positifs premiers entre eux et $n \geq 2$ un entier. Alors $a^n - b^n$ admet au moins un diviseur premier primitif (c'est-à-dire qui ne divise pas $a^i - b^i$ pour tout $1 \leq i \leq n-1$) à l'exception des deux cas suivants :

(i) $2^6 - 1^6$,

(ii) $n = 2$ et $a + b$ est une puissance de 2.

Théorème (Théorème de Zsigmondy bis)**.**
Soient $a > b \geq 1$ des entiers strictement positifs premiers entre eux et $n \geq 2$ un entier. Alors $a^n + b^n$ admet au moins un facteur premier qui ne divise pas $a^k + b^k$ pour tout $1 \leq k \leq n$, à l'exception du cas $2^3 + 1^3$.

- Exercices -

Exercice 1 Pour un entier $n \geq 2$, notons a_n le nombre entier dont l'écriture décimale comporte n fois le chiffre 1. Soit $n \geq 1$. Existe-t-il un nombre premier p divisant a_n mais pas $a_{n-1}, \ldots, a_1$?

Exercice 2 (Malaisie 2015) Trouver tous les entiers $x, y, z \geq 0$ tels que $2^x 3^y + 1 = 7^z$.

Exercice 3 Trouver tous les entiers $x, y \geq 0$ tels que $2 \cdot 3^x = 5^y + 1$.

Exercice 4 (Roumanie 2015) Trouver tous les entiers $x, y, z \geq 0$ tels que $21^x + 4^y = z^2$.

Exercice 5 Trouver tous les entiers $x, y, z \geq 0$ tels que $3^x + 11^y = z^2$.

Exercice 6 (Olympiades Italie 2003) Trouver tous les entiers strictement positifs (a, b, p) avec p premier tels que $2^a + p^b = 19^a$.

Exercice 7 (D'après olympiade Russie 1996) Trouver tous les entiers strictement positifs (x, y, n, k) tels que x et y soient premiers entre eux et $3^n = x^k + y^k$.

Exercice 8 (Olympiades Iran) Soit A un ensemble fini de nombres premiers et soit $a \geq 2$ un entier. Montrer qu'il n'existe qu'un nombre fini d'entiers positifs n tels que tous les facteurs premiers de $a^n - 1$ appartiennent à A.

Exercice 9 (D'après liste courte Olympiades Internationales de Mathématiques 2002) Soit $n \geq 1$ un entier et soient $p_1, p_2, \ldots, p_n$ des nombres premiers distincts tous supérieurs ou égaux à 5. Montrer que $2^{p_1 p_2 \cdots p_n} + 1$ a au moins 2^{2^n} diviseurs différents.

Exercice 10 (Liste courte Olympiades Internationales de Mathématiques 2004) Trouver tous les entiers strictement positifs a, m, n tels que $a^m + 1$ divise $(a+1)^n$.

Exercice 11 (Olympiades États-Unis 2001) Trouver tous les entiers strictement positifs x, r, p, n tels que p soit premier, $n, r > 1$ et $x^r - 1 = p^n$.

Exercice 12 (Compétition Tchéco-Slovaque 1996) Trouver tous les entiers strictement positifs x, y, p tels que $p^x - y^p = 1$ avec p premier.

Exercice 13 (Olympiade Pologne 2010) Soient q, p deux nombres premiers tels que $q > p > 2$. Montrer que $2^{pq} - 1$ a au moins trois facteurs premiers distincts.

Exercice 14 (Olympiade Japon 2011)Trouver tous les entiers strictement positifs a, n, p, q, r tels que $a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$.

Exercice 15 (Olympiades Balkaniques de Mathématiques 2009) Trouver tous les entiers strictement positifs x, y, z tels que $5^x - 3^y = z^2$.

Exercice 16 Trouver tous les nombres strictement positifs a, p, n tels que $p^a - 1 = 2^n(p-1)$, où p est un nombre premier.

Exercice 17 (Olympiade Estonie 2007) Soient $n, b \geq 2$ des entiers. Montrer que si $(b^n - 1)/(b-1)$ est une puissance d'un nombre premier, alors n est un nombre premier.

Exercice 18 Trouver tous les entiers strictement positifs a, m, n tels que $(a+1)(a^2+a+1)\cdots(a^n + a^{n-1} + \cdots + 1) = a^m + a^{m-1} + \cdots + 1$.

Exercice 19 (Olympiade Roumanie 1994) Montrer que la suite $a_n = 3^n - 2^n$ ne contient pas trois termes d'une même suite géométrique dont la raison est un entier au moins égal à 2.

Exercice 20 (Olympiade Angleterre 1996) Trouver les entiers positifs x, y, z tels que $2^x + 3^y = z^2$.

Exercice 21 Trouver toutes les solutions entières strictement positives de $x^{2009} + y^{2009} = 7^k$.

Exercice 22 Pour un entier $n \geq 2$, $3^n - 2^n$ est une puissance d'un nombre premier. Montrer que n est premier.

Exercice 23 (Liste courte Olympiades Internationales de Mathématiques 1997) Soient b, m, n des entiers strictement positifs avec $b > 1$ et $m \neq n$. Prouver que si $b^m - 1$ et $b^n - 1$ ont les même facteurs premiers, alors $b + 1$ est une puissance de 2.

Exercice 24 (Olympiade Iran 2006) Soient $a, b, c, k \geq 1$ des entiers. On pose $n = a^{c^k} - b^{c^k}$. Si c est divisible par au moins q nombres premiers différents, montrer que n est divisible par au moins qk nombres premiers différents.

Solution de l'exercice 1 On remarque que $a_n = (10^n - 1)/9$. Le théorème de Zsigmondy s'applique et fournit l'existence d'un nombre premier p divisant $10^n - 1$ mais aucun des nombres $10^{n-1} - 1, \ldots, 10^1 - 1$. En particulier, p ne divise pas 9, donc $p \neq 3$ ce qui montre que p divise a_n.

Solution de l'exercice 2 Si $z \geq 2$, le théorème de Zsigmondy fournit un diviseur premier p de $7^z - 1$ ne divisant pas $7 - 1 = 3 \cdot 2$. Donc $z \leq 2$. Réciproquement, on vérifie que $(x, y, z) = (1, 1, 1)$ et $(x, y, z) = (4, 1, 2)$ sont solutions.

Solution de l'exercice 3 Si $y \geq 2$, d'après le théorème de Zsigmondy, il existe un nombre premier p divisant $5^y + 1$ mais pas $5 + 1$. Donc $y \leq 1$. Réciproquement, $(x, y) = 1$ est bien solution.

Solution de l'exercice 4 Soit (x, y, z) une solution. On a clairement $x, y, z \geq 1$. On réécrit l'équation sous la forme $3^x \cdot 7^x = (z - 2^y)(z + 2^y)$. Comme $z - 2^y$ et $z + 2^y$ sont premiers entre eux (z est impair), on a deux cas à traiter :

(i) $z - 2^y = 1$ et $z + 2^y = 21^x$. Donc $2^{y+1} = 21^x - 1$, qui est divisble par 5, absurde.

(ii) $z - 2^y = 3^x$ et $z + 2^y = 7^x$. Alors $2^{y+1} = 7^x - 3^x$. Si $x \geq 2$, d'après le théorème de Zsigmondy, il existe un nombre premier p divisant $7^x - 3^x$ mais pas $7 - 3$. Donc $x = 1$. Réciproquement, on vérifie que $(x, y, z) = (1, 1, 5)$.

Solution de l'exercice 5 Modulo 3, on voit que y est pair. En écrivant $y = 2a$, on obtient $3^x = (z - 11^a)(z + 11^a)$. Comme $z - 11^a$ et $z + 11^a$ sont premiers entre eux, on peut écrire $z - 11^a = 3^b$ et $z + 11^a = 3^c$ avec $c \geq b$. Donc $3^c - 3^b = 2 \cdot 11^a$. On en déduit que $b = 0$. Puis, si $c \geq 2$, d'après le théorème de Zsigmondy, il existe un nombre premier p divisant $3^c - 1$ mais pas $3 - 1$. Donc $c = 1$ et $z = 2$ Réciproquement $(x, y, z) = (1, 0, 2)$ est solution.

Solution de l'exercice 6 On réécrit l'équation sous la forme $19^a - 2^a = p^b$. Comme 17 divise le terme de gauche, on a $p = 17$. D'après le théorème de Zsigmondy, si $a \geq 2$, il existe un nombre premier divisant $19^a - 2^a$ mais pas $19^1 - 2^1 = 17$, absurde. La seule solution est donc $(a, b, p) = (1, 1, 17)$.

Solution de l'exercice 7 Tout d'abord, k doit être impair. En effet si k était pair, x^k et y^k seraient des carrés et il est facile de vérifier $3|a^2 + b^2 \implies 3|a$ et $3|b$ (il suffit de vérifier toutes les congruences possibles mod 3 pour a et b). Si $(x, y, k) \neq (2, 1, 3)$ et $k > 1$, on peut appliquer le théorème de Zsigmondy, qui fournit un nombre premier p divisant $x^k + y^k$ mais pas $x + y$. Or $x + y$ divise $x^k + y^k$, ce qui implique que $x^k + y^k$ admet au moins deux diviseurs premiers. De plus, si $(x, y, k) = (2, 1, 3)$ alors $n = 2$, et si $k = 1$, on a simplement $3^n = x^1 + (3^n - x)$ avec $1 \leq x \leq 3^n - 1$ et $3 \nmid x$.

Les solutions sont donc $(x, y, n, k) = (2, 1, 2, 3)$, $(x, y, n, k) = (1, 2, 2, 3)$ et $(x, y, n, k) = (x, 3^n - x, n, 1)$ avec $n \geq 1$, $1 \leq x \leq 3^n - 1$ et $3 \nmid x$.

Solution de l'exercice 8 Soient $p_1, p_2, p_3, \ldots$ des nombres premiers impairs distincts. Posons $n_k = p_1 p_2 \cdots p_k$. En particulier, $a^{n_i} - 1$ divise $a^{n_j} - 1$ pour $i < j$. D'après le théorème de Zsigmondy, il existe un nombre premier q_k tel que q_k divise $a^{n_k} - 1$ mais ne divise pas $a^{n_i} - 1$ pour $1 \leq i \leq k$. En particulier, cela implique que les nombres premiers $q_k; k \geq 1$ sont tous différents, et cela conclut.

Solution de l'exercice 9 Posons $N = 2^{p_1 p_2 \cdots p_n} + 1$. On va montrer que N a au moins 2^n facteurs premiers distincts, ce qui impliquera que N a au moins $2^{2^n} \geq 4^n$ diviseurs. Soit $A \subset \{1, 2, \ldots, n\}$ et posons $N_A = 2^{\prod_{i \in A} p_i} + 1$, avec la convention $N_\emptyset = 3$. Alors N_A divise N. D'après le théorème de Zsigmondy (qu'on peut utiliser car l'exception $2^3 + 1$ ne peut arriver puisque $p_i \geq 5$), il existe un nombre premier q_A divisant N_A et ne divisant pas $2^j + 1$ pour $1 \leq j < \prod_{i \in A} p_i$ si $A \neq \emptyset$. De plus, on voit que $q_A \neq q_{A'}$ si $A \neq A'$. Comme il existe 2^n sous-ensembles de $\{1, 2, \ldots, n\}$, cela conclut.

Solution de l'exercice 10 Comme $m = 1$ convient pour tous entiers $a, n > 0$, on peut supposer $m > 1$. Comme $a = 1$ convient pour tous entiers $m, n > 0$, on peut supposer $a > 1$.

Si $(a, m) \neq (2, 3)$, le théorème de Zsigmondy implique qu'il existe un facteur premier de $a^m + 1$ qui ne divise pas $a + 1$ et donc $(a + 1)^n$.

Si $(a, m) = (2, 3)$, on voit que seuls les entiers $n \geq 2$ sont solution.

Solution de l'exercice 11 Si les hypothèses du théorème de Zsigmondy sont remplies, il existe un facteur premier de $x^r - 1$ qui ne divise pas $x - 1$. Comme $x - 1$ divise $x^r - 1$, ceci implique que $x^r - 1$ admet au moins deux facteurs premiers et ne peut donc pas être une puissance d'un nombre premier.

Il reste donc à traiter les deux cas suivants :

(i) $(x, r) = (2, 6)$ (qui ne convient pas),

(ii) $r = 2$ et $x + 1$ est une puissance de 2. Dans ce cas $(x - 1)(x + 1) = p^n$, ce qui donne aisément $p = 2$ et $x = 3$.

Solution de l'exercice 12 Réécrivons l'équation sous la forme $y^p + 1^p = p^x$. Si $y = 1$, on voit que $p = 2$ et $x = 1$. Si $p = 2$, il vient aisément que nécessairement $x, y = 1$. On suppose donc p impair de sorte que $y + 1$ divise $y^p + 1$.

Si les hypothèses du théorème de Zsigmondy sont remplies, il existe un facteur premier de $y^p + 1$ qui ne divise pas $y + 1$, de sorte que $y^p + 1$ ne peut pas être une puissance d'un nombre premier. Il reste donc à traiter le cas $(y, p) = (2, 3)$ qui donne la solution $x = 2$.

Solution de l'exercice 13 Les entiers $2^p - 1$ et $2^q - 1$ divisent $2^{pq} - 1$. D'après le théorème de Zsigmondy, $2^{pq} - 1$ a un facteur premier p_1 qui ne divise ni $2^p - 1$, ni $2^q - 1$. De même, $2^q - 1$ admet un facteur premier p_2 qui ne divise pas $2^p - 1$, et $2^p - 1$ admet un facteur premier p_3. De plus, par construction, p_1, p_2, p_3 sont distincts.

Solution de l'exercice 14 Comme $a = 1$ est solution, supposons maintenant $a \geq 2$. Il est clair qu'alors $n \geq p, q, r \geq 1$.

Si l'un des entiers p, q, r est égal à n, on a $a = 2$ et les deux autres sont égaux à 1. On trouve donc les solutions $(a, n, p, q, r) = (2, n, 1, 1, n), (2, n, 1, n, 1), (2, n, n, 1, 1)$. On suppose dans la suite que $p, q, r < n$.

Si les hypothèses du théorème de Zsigmondy sont remplies, alors $a^n - 1$ admet un diviseur premier qui ne divise aucun des entiers $a^p - 1, a^q - 1, a^r - 1$, et on ne peut donc pas avoir $a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$.

Sinon, on a soit :

(i) $n = 2$ et $a = 2^s - 1$. Dans ce cas, comme on a supposé $p, q, r < n$, on a $p = q = r = 1$, et $a^2 - 1 = (a - 1)^3$. Ceci implique $a = 3$ et on trouve la solution $(a, n, p, q, r) = (3, 2, 1, 1, 1)$.

(ii) $a = 2$ et $n = 6$. Dans ce cas, on trouve aisément les solutions $(a, n, p, q, r) = (2, 6, 2, 2, 3), (2, 6, 2, 3, 2), (2$

Solution de l'exercice 15 En regardant modulo 3, on voit que x est pair. On écrit $x = 2w$, de sorte que

$$3^y = 5^{2w} - z^2 = (5^w - z)(5^w + z).$$

De plus, PGCD$(5^w - z, 5^w + z)$=PGCD$(z, 5^w) = 1$. On a donc nécessairement $5^w - z = 1$ et $5^w + z = 3^a$. En additionnant les deux égalités, il vient $3^a + 1 = 2 \cdot 5^w$. Pour $a = 2$, on a $w = 1$ ce qui donne la solution $(x, y, z) = (2, 2, 4)$. Si $a \geq 3$, d'après le théorème de Zsigmondy, $3^a + 1$ a un facteur premier p qui ne divise pas $3^2 + 1$, ce qui implique $p \neq 2, 5$. Il n'y a donc pas de solutions dans ce cas.

Solution de l'exercice 16 Il est clair que $p > 2$. Supposons par l'absurde que $a = uv$ soit composé. Alors d'après le théorème de Zsigmondy, $p^u - 1$ a un facteur premier q qui ne divise pas $p - 1$. Or $p^u - 1$ divise $p^a - 1 = 2^n(p - 1)$. On a donc $q = 2$. Or $p - 1$ est pair, absurde. Donc a est premier.

Si $a = 2$, on trouve que $p = 2^n - 1$.

Si $a > 2$, de même, le théorème de Zsigmondy implique que $2^n(p - 1) = p^a - 1$ admet un facteur premier r qui ne divise pas $p - 1$. Ceci implique que $r = 2$, absurde car $p - 1$ est pair.

Les solutions sont donc $a = 2$ et n tel que $2^n - 1$ soit premier.

Solution de l'exercice 17 On vérifie d'abord que $(b, n) = (2, 6)$ ne convient pas. Ensuite, par l'absurde, supposons que n ne soit pas un nombre premier et choisissons un diviseur $1 < d < n$ de n. Écrivons $b^n - 1 = p^k(b - 1)$ et appliquons le théorème de Zsigmondy : il existe nombre premier q divisant $b^n - 1$ mais ne divisant ni $b - 1$, ni $b^d - 1$, ce qui implique $p = q$. Ainsi $p \nmid b^d - 1$, et $\frac{b^d-1}{b-1} \mid \frac{b^n-1}{b-1} = p^k$, ce qui est absurde.

Solution de l'exercice 18 Supposons que $(m, n) \neq (1, 1)$ (qui convient clairement), et aussi que $a > 1$ (si $a = 1$ on a la solution $(a, m, n) = (1, (n + 1)! - 1, n)$). On a alors $m > n$, et on peut écrire l'équation sous la forme équivalente suivante :

$$\frac{a^2 - 1}{a - 1} \cdot \frac{a^3 - 1}{a - 1} \cdots \frac{a^{n+1} - 1}{a - 1} = \frac{a^{m+1} - 1}{a - 1},$$

ou encore

$$(a^2 - 1)(a^3 - 1) \cdots (a^{n+1} - 1) = (a^{m+1} - 1)(a - 1)^{n-1}.$$

Si les hypothèses du théorème de Zsigmondy sont remplies, il existe un facteur premier de $a^{m+1} - 1$ qui ne divise aucun des entiers $a^2 - 1, a^3 - 1, \ldots, a^{n+1} - 1$. Comme $m + 1 > 2$, il reste donc à traiter le cas $(a, m + 1) = (2, 6)$, autrement dit $a = 2$ et $m = 5$. Dans ce cas, $3 \cdot 7 \cdot 15 \cdots (2^{n+1} - 1) = 63$, qui ne fournit pas d'autre solution.

Solution de l'exercice 19 Raisonnons par l'absurde en supposant que a_r, a_s, a_t appartiennent à une suite géométrique de raison $b \geq 2$, avec $r < s < t$. Alors

$$(3^r - 2^r)b^k = 3^s - 2^s, \qquad (3^s - 2^s)b^l = 3^t - 2^t \tag{1}$$

avec $k, l \geq 1$. D'après le théorème Zsigmondy, il existe un nombre premier p divisant $3^t - 2^t$ mais pas $3^s - 2^s$. D'après la deuxième égalité de (1), p divise b. D'après la première égalité de (1), p divise alors $3^s - 2^s$, absurde.

Solution de l'exercice 20 Si $x = 0$, on vérifie que $y = 1, z = 2$ et que si $y = 0$, $x = 3$ et $z = 3$. On suppose donc $x, y \geq 1$. La suite est proche de l'exercice 15. Modulo 3, on voit que x est impair. Écrivons donc $x = 2w$, de sorte que $3^y = z^2 - 2^{2w} = (z - 2^w)(z + 2^w)$. Le PGCD de $z - 2^w$ et de $z + 2^w$ est égal au PGCD de z et de 2^w, qui vaut 1. Ainsi $z - 2^w = 1$ et $z + 2^w = 3^y$. En soustrayant ces deux égalités, il vient $2^{w+1} = 3^y - 1$. Si $y \neq 2$, alors $y \geq 3$ et le théorème de Zsigmondy assure l'existence d'un nombre premier p divisant $3^y - 1 = 2^{w+1}$ mais pas $3^1 - 1 = 2$, absurde. Si $y = 2$, on trouve la solution $(x, y, z) = (4, 2, 5)$.

Solution de l'exercice 21 Comme $2009 = 49 \cdot 41$, $x^{49} + y^{49}$ divise $x^{2009} + y^{2009}$. D'après le théorème de Zsigmondy, il existe un nombre premier divisant $x^{49} + y^{49}$ mais pas $x + y$. Comme $x + y$ divise $x^{2009} + y^{2009}$, on en déduit que $x^{2009} + y^{2009}$ admet au moins deux facteurs premiers, absurde.

Solution de l'exercice 22 Comme dans la solution précédente de l'exercice **??**, on commence par montrer que si $n > 2$ et $3^n - 2^n = p^k$ pour $k \geq 1$, alors n est impair. Supposons par l'absurde $n = ab$ composé. Alors $(3^a)^b - (2^a)^b = p^k$. Comme n est impair, on a $b > 2$ et on peut appliquer le théorème de Zsigmondy : il existe un nombre premier q divisant $3^n - 2^n$ mais pas $3^a - 2^a$. En considérant un diviseur premier de $3^a - 2^a$, on voit que $3^n - 2^n$ admet deux diviseurs premiers distincts, absurde.

Solution de l'exercice 23 Par symétrie, supposons $n > m$. Si les hypothèses du théorème de Zsigmondy sont remplies, il existe un facteur premier de $b^n - 1$ qui ne divise pas $b^m - 1$. Ainsi $b^m - 1$ et $b^n - 1$ ne peuvent pas avoir les mêmes facteurs premiers.

Il reste donc à traiter les deux cas suivants :

(i) $(b, n) = (2, 6)$. On vérifie que cela ne donne pas de solution pour m ;

(ii) $n = 2$ et $b + 1$ est une puissance de 2, ce qui était demandé.

Solution de l'exercice 24 Notons q le nombre de diviseurs premiers de c. Supposons d'abord $q = 1$, de sorte que c est premier. Si $k = 1$, il n'y a rien à faire. Sinon, si $c \neq 2$, on peut appliquer le théorème de Zsigmondy avec $a^i - b^i$ pour chaque diviseur i de c^k, ce qui nous fournit même $k + 1$ diviseurs premiers différents de $a^{c^k} - b^{c^k}$. Si $c = 2$, on écrit $a^{2^k} - b^{2^k} = (a^{2^{k-1}} - b^{2^{k-1}})(a^{2^{k-1}} + b^{2^{k-1}})$. On applique alors le théorème de Zsigmondy avec $a^i + b^i$ pour chaque diviseur i de 2^{k-1}, ce qui nous fournit k diviseurs premiers différents de $a^{2^k} - b^{2^k}$.

Supposons maintenant $q \geq 2$. On appliquer alors le théorème de Zsigmondy avec $a^i - b^i$ pour chaque diviseur i de c^k autre que 2 et 6, ce qui nous donne au moins $(k + 1)^q - 2 \geq kq$ diviseurs premiers différents de $a^{c^k} - b^{c^k}$.

Solution de l'exercice 25 Il suffit de trouver une infinité de couples de nombres premiers distincts (p, q) tels que $p \mid 2^{q-1} - 1$ et $q \mid 2^{p-1} - 1$.

Soit p un nombre premier tel que $p \equiv 3 \pmod 8$. Posons $n = (p - 1)/2$. Alors d'après le théorème de Zsigmondy, il existe un nombre premier $q > 2$ tel que l'ordre de 2 modulo q vaut $(p - 1)/2$. Comme p est congru à 3 modulo 8, p n'est pas un carré modulo 8, ce qui implique par réciprocité quadratique que 2 n'est pas un carré modulo p. Ceci implique que l'ordre de 2 modulo p est différent de $(p - 1)/2$, et donc $p \neq q$. De plus, par cosntruction, q divise $2^{p-1} - 1$.

Notons ω_p et ω_q les ordres respectifs de 2 modulo p et q. D'après le petit théorème de Fermat, $(p-1)/2 = \omega_q \mid q-1$. Comme $q-1$ est pair et que $(p-1)/2$ est impair, on en déduit que $p-1 \mid q-1$. D'autre part, d'après le petit théorème de Fermat, $\omega_p \mid p-1 \mid q-1$. Donc $\omega_p \mid q-1$, ce qui implique $2^{q-1} \equiv 1 \pmod{p}$. Ceci conclut.