Autour des diviseurs premiers de $a^n \pm b^n$

Igor Kortchemski*

Résumé

Nous nous intéressons à plusieurs propriétés des diviseurs premiers de $a^n \pm b^n$. En particulier, en utilisant les polynômes cyclotomiques, nous démontrons le théorème de Zsigmondy, qui s'intéresse aux diviseurs premiers de $a^n - b^n$ ne divisant aucun des entiers $a^j - b^j$ pour $1 \leqslant j < n$. Les notions abordées sont illustrées par de nombreux exercices issus de diverses olympiades de mathématiques.

1 Introduction

Ce texte présente des résultats concernant l'étude des facteurs premiers de $a^n \pm b^n$ autour de quatre thèmes. Nous commençons par démontrer le résultat suivant, où pour un entier relatif non nul $n \in \mathbb{Z}$ et un nombre premier p, on note $v_p(n)$ l'exposant de la plus grande puissance de p divisant n.

Théorème 1 (Théorème « Lifting The Exponent » (LTE))**.** *Soit p un nombre premier **impair**. Soient a, b des nombres entiers relatifs distincts et un entier $n \geqslant 1$. On suppose que p divise $a - b$ mais que $p \nmid a, p \nmid b$. Alors :*

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

Si ce théorème, redécouvert de nombreuses fois, fait partie du « folklore » mathématique, il semble qu'il apparaisse en 1878 dans les travaux de Lucas [6, Section XIII] (avec une petite erreur dans le cas $p = 2$), alors professeur au lycée Charlemagne. Il est maintenant popularisé sous le nom de « Théorème LTE ».

Nous poursuivons par des propriétés de l'ordre multiplicatif d'un entier dans $\mathbb{Z}/n\mathbb{Z}$, qui est souvent utile pour étudier des questions de divisibilité.

Nous définissons ensuite les polynômes cyclotomiques et étudions en particulier des propriétés concernant leurs diviseurs premiers en lien avec l'ordre multiplicatif.

Finalement, si $a, b \in \mathbb{Z}$ et $n \geqslant 2$ est un entier, nous étudions la question de l'existence de diviseurs premiers primitifs de $a^n - b^n$. Par définition, un diviseur premier p de $a^n - b^n$ est dit *primitif* si, pour tout entier $1 \leqslant j < n$, p ne divise pas $a^j - b^j$, et *non primitif* sinon. Par exemple, 5 est un diviseur primitif de $2^4 - 1^4$, 3 n'est pas diviseur primitif de $2^4 - 1^4$, et $2^6 - 1^6$ n'admet pas de diviseur premier primitif. En utilisant le théorème LTE ainsi que les polynômes cyclotomiques, nous démontrons enfin le théorème de Zsigmondy, qui garantit l'existence de diviseurs premiers primitifs, sauf exceptions.

Théorème 2 (Théorème de Zsigmondy)**.** *Soient $a > b \geqslant 1$ des entiers premiers entre eux et $n \geqslant 2$ un entier. Alors $a^n - b^n$ admet au moins un diviseur premier primitif à l'exception des deux cas suivants :*

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

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

Ce résultat est dû à Bang [3] (1886) dans le cas $b = 1$, et Zsigmondy [10] (1892) dans le cas général. Ce théorème a été redécouvert plusieurs fois avec des variantes de preuve, par exemple par Birkhoff & Vandiver [4] en 1904, Dickson [5] en 1905 (dans le cas $b = 1$) et Artin [2] en 1955. Cependant, toutes ces preuves utilisent les polynômes cyclotomiques.

Ce théorème implique que hors cas exceptionnels (i) et (ii), $a, n \geqslant 2$ étant fixés, il existe un nombre premier p tel que l'ordre de a modulo p vaut n (voir la Définition 1 ci-dessous pour la définition de l'ordre). Il est aussi intéressant de noter que la démonstration de Wedderburn du théorème éponyme [7], qui dit que tout corps fini est commutatif, utilise le théorème de Bang. Mentionnons également que le théorème de Zsigmondy trouve des applications dans la théorie des groupes finis (voir par exemple [2]).

*DMA, École Normale Supérieure, Paris igor.kortchemski@normalesup.org

À la fin des quatre parties relatives respectivement au théorème LTE, à l'ordre multiplicatif dans $\mathbb{Z}/n\mathbb{Z}$, aux polynômes cyclotomiques et au théorème de Zsigmondy se trouvent des exercices issus de diverses olympiades de mathématiques (de niveau lycée) afin d'illustrer ces notions, et dont les solutions figurent en fin de texte. Si bien entendu des solutions différentes sans les deux derniers outils avancés existent, nous verrons que ceux-ci fournissent peut-être des approches plus naturelles.

2 Théorème LTE

2.1 Preuve du théorème

On commence par le lemme suivant.

Lemme 1. *Soient x, y des entiers relatifs distincts et $n \geqslant 1$. Soit p un nombre premier ne divisant pas n, tel que $p \mid x - y$ mais tel que $p \nmid x, p \nmid y$. Alors*

$$v_p(x^n - y^n) = v_p(x - y).$$

Démonstration. On écrit $x^n - y^n = (x-y)(x^{n-1} + yx^{n-2} + \cdots + y^{n-1})$. Comme $x \equiv y \pmod p$, on remarque que $x^{n-1} + yx^{n-2} + \cdots + y^{n-1} \equiv nx^{n-1} \pmod p$. Comme p ne divise ni x, ni y, il s'ensuit que $nx^{n-1} \not\equiv 0 \pmod p$ (et, en particulier, $x^n \neq y^n$). Donc p ne divise pas $x^{n-1} + yx^{n-2} + \cdots + y^{n-1}$ et le résultat en découle. □

Nous sommes maintenant en mesure d'établir le théorème LTE.

Preuve du Théorème 1. **Étape 1.** On montre d'abord que

$$v_p(a^p - b^p) = v_p(a - b) + 1. \tag{1}$$

À cet effet, notons $A = a^{p-1} + ba^{p-2} + \cdots + b^{p-1}$. Le même raisonnement que dans la preuve du Lemme 1 fournit $A \equiv pa^{p-1} \equiv 0 \pmod p$. Étudions maintenant A modulo p^2. Comme p divise $a - b$, il existe $k \in \mathbb{Z}$ tel que $b = a + kp$. Alors, tout entier $0 \leqslant i \leqslant p-1$, on a

$$b^i a^{p-1-i} = (a+kp)^i a^{p-1-i} = \left(a^i + ikpa^{i-1} + \sum_{j=2}^{i} \binom{i}{j} (kp)^j a^{i-j} \right) a^{p-1-i} \equiv a^{p-1} + ikpa^{p-2} \pmod{p^2}.$$

Il en découle que

$$\begin{aligned} \sum_{i=0}^{p-1} b^i a^{p-1-i} &\equiv \sum_{i=0}^{p-1} \left(a^{p-1} + ikpa^{p-2}\right) \pmod{p^2} \\ &\equiv pa^{p-1} + \frac{p-1}{2} \cdot kp^2 a^{p-2} \pmod{p^2} \quad \left(\frac{p-1}{2} \text{ est entier car } p \text{ est impair}\right) \\ &\equiv pa^{p-1} \pmod{p^2} \not\equiv 0 \pmod{p^2} \quad (\text{car } p \nmid a). \end{aligned}$$

Ceci établit (1).

Étape 2. Par une récurrence immédiate, on obtient que

$$v_p(a^{p^i} - b^{p^i}) = v_p(a - b) + i. \tag{2}$$

pour tout entier $i \geqslant 1$. Écrivons à présent $n = p^\alpha N$ avec p ne divisant pas N. Alors

$$v_p(a^n - b^n) = v_p\left(\left(a^{p^\alpha}\right)^N - \left(b^{p^\alpha}\right)^N\right) = v_p(a^{p^\alpha} - b^{p^\alpha}) = v_p(a-b) + \alpha,$$

où on a utilisé le Lemme 1 pour l'avant-dernière égalité et (2) pour la dernière égalité. □

Lorsque n est impair, en changeant b en $-b$ on en déduit immédiatement le résultat suivant.

Théorème 3 (Théorème LTE bis)**.** *Soit p un nombre premier **impair**. Soient a, b des nombres entiers (non nécessairement positifs) et un entier $n \geqslant 1$* impair *. On suppose que p divise $a + b$ mais que p ne divise ni a ni b. Alors $v_p(a^n + b^n) = v_p(a+b) + v_p(n)$.*

Nous encourageons le lecteur à étudier le cas $p = 2$.

Voici un exemple d'application : trouver tous les nombres premiers p tels que $(p-1)^p + 1$ soit une puissance de p.

Pour répondre à cette question, 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.

2.2 Exercices

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

Exercice 3 (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 4 Trouver toutes les solutions entières strictement positives de $x^{2009} + y^{2009} = 7^k$.

Exercice 5 (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.

3 Un lemme utile

On établit ici le lemme utile suivant (qui est probablement un résultat bien connu lorsque $b = 1$) :

Lemme 2. *Soient $a \neq b$ des entiers relatifs premiers entre eux. Soient $m, n \geqslant 1$ des entiers. Alors*

$$\mathrm{PGCD}\,(a^n - b^n, a^m - b^m) = \left|a^{\mathrm{PGCD}(m,n)} - b^{\mathrm{PGCD}(m,n)}\right|.$$

Démonstration. On montre que chaque terme de l'égalité divise l'autre. Pour simplifier les notations, posons $V_n = a^n - b^n$ pour $n \geqslant 1$. Tout d'abord, comme $\mathrm{PGCD}\,(m, n)$ divise m, $V_{\mathrm{PGCD}(m,n)}$ divise V_m. De même, $V_{\mathrm{PGCD}(m,n)}$ divise V_n. On en déduit que $V_{\mathrm{PGCD}(m,n)}$ divise $\mathrm{PGCD}\,(V_m, V_n)$.

Ensuite, si $m = n$, il n'y a rien à faire. Sinon, supposons $m > n$. On vérifie que

$$a^m - b^m - (a^n - b^n) = a^n(a^{m-n} - b^{m-n}) + (a^n - b^n)(b^{m-n} - 1) = a^n V_{m-n} + V_n(b^{m-n} - 1).$$

Il en découle que $\mathrm{PGCD}\,(V_m, V_n)$ divise $a^n V_{m-n}$. Comme a et b sont premiers entre eux, $\mathrm{PGCD}\,(V_m, V_n)$ divise V_{m-n}. Ainsi, $\mathrm{PGCD}\,(V_m, V_n)$ divise $\mathrm{PGCD}\,(V_{m-n}, V_n)$.

Si $m < n$, on montre de même que $\mathrm{PGCD}\,(V_m, V_n)$ divise $\mathrm{PGCD}\,(V_{n-m}, V_n)$. Or on sait que $\mathrm{PGCD}\,(m - n, n) = \mathrm{PGCD}\,(m, n - m) = \mathrm{PGCD}\,(m, n)$. Par récurrence (par exemple sur $m + n$) on en déduit que $\mathrm{PGCD}\,(V_m, V_n)$ divise $\mathrm{PGCD}\,(m, n)$, ce qui conclut. □

4 Ordre multiplicatif d'un entier

4.1 Définition

Dans cette partie, on considère $a \in \mathbb{Z}$ et $n \geqslant 1$ des entiers premiers entre eux.

Définition 1. *L'ordre de a modulo n est le le plus petit entier non nul, noté $\omega_n(a)$, tel que $a^{\omega_n(a)} \equiv 1 \pmod{n}$.*

Cette définition a un sens, car il existe bien un entier $k \geqslant 1$ tel que $a^k \equiv 1 \pmod{n}$. En effet, comme l'ensemble des résidus modulo n est fini, il existe deux entiers distincts $1 \leqslant r < s$ tels que $a^s \equiv a^r \pmod{n}$. Alors n divise $a^r(a^{s-r} - 1)$, donc aussi $a^{s-r} - 1$ car a et n sont premiers entre eux.

L'utilité de cette notion provient essentiellement du théorème suivant, dont la preuve est laissée au lecteur :

Théorème 4. *Soient a, n des entiers naturels premiers entre eux et $k \geqslant 1$ un entier vérifiant $a^k \equiv 1 \pmod{n}$. Alors $\omega_n(a)$ divise k.*

Dans la suite, ϕ désigne la fonction indicatrice d'Euler. On rappelle que $\phi(n)$ est le nombre d'entiers, compris au sens large entre 1 et n, premiers avec n, que $\phi(ab) = \phi(a)\phi(b)$ lorsque a et b sont des entiers premiers entre eux, et que $a^{\phi(n)} \equiv 1 \pmod{n}$ (théorème d'Euler). En particulier, $\omega_n(a)$ divise $\phi(n)$ (ce qui, dans le cas où $n = p$ est premier, donne $\omega_p(a) \mid p-1$). Ceci est en particulier utile lorsqu'on cherche l'ordre d'un entier modulo n à la main : il suffit de tester les diviseurs de $\phi(n)$.

Voici un exemple d'application.

(i) Trouver tous les entiers $n \geqslant 1$ tels que n divise $2^n - 1$.

(ii) Trouver tous les entiers $n \geqslant 1$ impairs tels que n divise $3^n + 1$.

Solution.

(i) Soit $n > 1$ tel que n divise $2^n - 1$. Il est clair que n est impair. Soit p le plus petit facteur premier de n, qui est donc impair. Alors $2^n \equiv 1 \pmod{p}$. Soit ω l'ordre de 2 modulo p. Alors ω divise n. D'autre part, d'après le petit théorème de Fermat, $2^{p-1} \equiv 1 \pmod{p}$. Ainsi ω divise $p-1$. D'après la condition sur p, on a nécessairement $\omega = 1$. Alors $2 \equiv 1 \pmod{p}$, ce qui est absurde. On a donc $n = 1$.

(ii) Soit $n > 1$ tel que n divise $3^n + 1$. Soit p le plus petit facteur premier de n, qui est donc impair, de sorte que $p > 3$. Alors $3^{2n} \equiv 1 \pmod{p}$. Soit ω l'ordre de 3 modulo p. Alors ω divise $2n$. D'autre part, d'après le petit théorème de Fermat, $3^{p-1} \equiv 1 \pmod{p}$. Ainsi ω divise $p-1$. On en déduit que ω divise $\mathrm{PGCD}(2n, p-1)$. D'après la condition sur p, on a nécessairement $\omega = 1$ ou 2. Dans le premier cas, $3 \equiv 1 \pmod{p}$ et donc $p = 2$, ce qui est exclu. Dans le deuxième cas, $3^2 \equiv 1 \pmod{p}$ et donc p divise 8, ce qui est exclu également. On en déduit que $n = 1$.

Pour les exercices qui suivent, il peut être utile de se rappeler que si a et n sont des entiers premiers entre eux, alors il existe un entier b tel que $ab \equiv 1 \pmod{n}$.

4.2 Exercices

Exercice 6 Existe-t-il des entiers $n \geqslant 1$ tels que 9 divise $7^n + n^3$?

Exercice 7 Trouver tous les entiers $m, n \geqslant 1$ tels que mn divise $3^m + 1$ et mn divise $3^n + 1$.

Exercice 8 Soient p, q deux nombres premiers tels que q divise $3^p - 2^p$. Montrer que p divise $q - 1$.

Exercice 9 (Olympiade Chine 2006) Trouver les entiers $a, n \geqslant 1$ tels que n divise $((a+1)^n - a^n)$.

Exercice 10 Soient $a, b > 1$ impairs tels que $a + b = 2^\alpha$ avec $\alpha \geqslant 1$. Montrer qu'il n'y a pas d'entiers $k > 1$ tels que k^2 divise $a^k + b^k$.

Exercice 11 Trouver tous les entiers n tels que 19 divise $2^{3n+4} + 3^{2n+1}$.

Exercice 12 Soient a, b, n des nombres entiers strictement positifs avec $a > b$. Montrer que n divise $\phi(a^n - b^n)$.

Exercice 13 Soient $n, k \geqslant 2$ des entiers tels que n divise $k^n - 1$. Peut-on avoir $\mathrm{PGCD}(n, k-1) = 1$?

Exercice 14 Soient x et y deux entiers positifs premiers entre eux. Si k est un entier impair positif qui divise $x^{2^n} + y^{2^n}$ avec $n \geqslant 1$, alors il existe un entier m tel que $k = 2^{n+1}m + 1$.

Exercice 15 Trouver tous les p, q premiers tels que pq divise $2^p + 2^q$.

Exercice 16 (Olympiade Irlande 1996) Soient p un nombre premier et a, n des entiers strictement positifs. Prouver que si $2^p + 3^p = a^n$, alors nécessairement $n = 1$.

Exercice 17 Soit $n > 1$ un entier impair. Si $m \geqslant 1$ est un entier, montrer que n ne divise pas $m^{n-1} + 1$.

Exercice 18 (Olympiades Internationales de Mathématiques 1990) Trouver tous les entiers $n \geqslant 1$ tels que n^2 divise $2^n + 1$.

Exercice 19 (Olympiade Bulgarie 1997) Pour un entier $n \geqslant 2$, $3^n - 2^n$ est une puissance d'un nombre premier. Montrer que n est premier.

Exercice 20 (Olympiade États-Unis 2003) Trouver tous les nombres premiers p, q, r tels que p divise $1 + q^r$, q divise $1 + r^p$ et r divise $1 + p^q$.

5 Polynômes cyclotomiques

Avant d'introduire les polynômes cyclotomiques, nous introduisons les racines primitives de l'unité et la fonction de Möbius.

5.1 Racines primitives de l'unité

Définition 2. *Soit $n \geqslant 1$ un entier. Un nombre complexe z tel que $z^n = 1$ est appelé racine n-ième de l'unité. Il y a n racines n-ièmes de l'unité : ce sont les n nombres complexes $e^{2i\pi k/n}$ pour $0 \leqslant k \leqslant n-1$. S'il existe un entier n tel que z est racine n-ième de l'unité, on dit simplement que z est racine de l'unité.*

Si z est une racine de l'unité, le plus petit entier $k \geqslant 1$ tel que $z^k = 1$ est appelé ordre de z, et est noté $\mathrm{ord}(z)$. *Si un nombre complexe z, racine de l'unité, est d'ordre k, on dit que z est une racine primitive k-ième (de l'unité).*

Nous mentionnons la propriété utile suivante, dont la démonstration est laissée au lecteur.

Proposition 1. *Soit z une racine de l'unité. Alors* $\mathrm{ord}(z^k) = \dfrac{\mathrm{ord}(z)}{\mathrm{PGCD}\,(k, \mathrm{ord}(z))}$. *En particulier, si z est une racine primitive n-ième, alors z^k est une racine primitive $n/\mathrm{PGCD}\,(k,n)$-ième.*

En utilisant ce résultat, il est possible d'en déduire qu'il existe $\phi(n)$ racines n-ièmes de l'unité.

5.2 Fonction de Möbius

Définition 3. *Soit $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ la fonction définie comme suit :*

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n \text{ est le produit de } k \text{ nombres premiers distincts} \\ 0 & \text{sinon.} \end{cases}$$

La fonction μ est appelée fonction de Möbius, et on remarque que $\mu(ab) = \mu(a)\mu(b)$ si a et b sont premiers entre eux. L'utilité de la fonction de Möbius provient, entre autres, du théorème d'inversion suivant, dont la preuve est laissée au lecteur.

Théorème 5 (Inversion multiplicative de Möbius)**.** *Soient $F, f : \mathbb{N}^* \to \mathbb{R}^*$ deux fonctions telles que $F(n) = \prod_{d \mid n} f(d)$ pour tout entier $n \geqslant 1$. Alors $f(n) = \prod_{d \mid n} F\left(\frac{n}{d}\right)^{\mu(d)}$ pour tout entier $n \geqslant 1$.*

Mentionnons qu'il existe une formule similaire d'inversion « additive » de Möbius.

5.3 Définition et premières propriétés

Définition 4. *Pour tout entier $n \geqslant 1$, on pose*

$$\Phi_n(X) = \prod_{z \text{ est racine primitive } n\text{-ième de l'unité}} (X - z)\,.$$

Le polynôme Φ_n, de coefficient dominant égal à 1, a priori à coefficients complexes, est appelé n-ième polynôme cyclotomique. Rappelons deux propriétés bien connues des polynômes cyclotomiques :

Théorème 6. *Pour tout entier $n \geqslant 1$,*

(i) on a $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$;

(ii) le polynôme Φ_n est à coefficients entiers.

Mentionnons ensuite deux corollaires immédiats du Théorème 6, mais utiles.

Corollaire 1. *Soit $n \geqslant 1$ un entier.*

(i) On a $n = \sum_{d \mid n} \phi(d)$.

(ii) Soient $a \in \mathbb{Z}$ et p un nombre premier. Si $p \mid a^n - 1$, alors il existe un diviseur d de n tel que $p \mid \Phi_d(a)$.

Le théorème 6 permet également d'obtenir différentes formules faisant intervenir des polynômes cyclotomiques :

Proposition 2. *(i) Si $n \geqslant 1$ est impair, on a $X^n + 1 = \prod_{d \mid n} \Phi_{2d}(X)$.*

(ii) Pour tout entier $n \geqslant 1$, on a $\Phi_n(X) = \prod_{d \mid n} \left(X^{\frac{n}{d}} - 1\right)^{\mu(d)}$.

(iii) Si p est un nombre premier et $n \geqslant 1$ un entier, on a $\Phi_{pn}(X) = \begin{cases} \Phi_n(X^p) & \text{si } p \mid n \\ \dfrac{\Phi_n(X^p)}{\Phi_n(X)} & \text{si } p \nmid n. \end{cases}$

(iv) Si $n \geqslant 3$ est un entier impair, alors $\Phi_{2n}(X) = \Phi_n(-X)$.

(v) Si $a, n \geqslant 1$ sont des entiers premiers entre eux, alors $\Phi_n(X^a) = \prod_{d \mid a} \Phi_{nd}(X)$.

Démonstration. Pour (i), d'après le Théorème 6 (i), on a

$$(X^n - 1)(X^n + 1) = X^{2n} - 1 = \prod_{d \mid 2n} \Phi_d(X) = \prod_{d \mid n} \Phi_d(X) \cdot \prod_{d \mid n} \Phi_{2d}(X) = (X^n - 1) \cdot \prod_{d \mid n} \Phi_{2d}(X),$$

d'où le résultat en divisant par $X^n - 1$.

Compte tenu du Théorème 6 (i), la seconde assertion est une conséquence immédiate du théorème 5.

La troisième assertion découle aisément de la seconde, et on laisse les détails au lecteur.

D'après (iii) on a $\Phi_{2n}(X) = \Phi_n(X^2)/\Phi_n(X)$. Or si $n \geqslant 3$ est impair, on a $\Phi_n(X^2) = \Phi_n(X) \cdot \Phi_n(-X)$. En effet, si z^2 est racine n-ième de l'unité, on vérifie aisément que soit z soit $-z$ est racine n-ième de l'unité, ce qui fournit (iv) puisque $\Phi_n(-X)$ est unitaire, tout comme $\Phi_{2n}(X)$.

Pour la dernière assertion, en utilisant le Corollaire 1 (i), on vérifie que les degrés des deux polynômes unitaires sont les mêmes. Il suffit donc de montrer que si z^a est une racine primitive n-ième, il existe un diviseur d de a tel que $\Phi_{nd}(z) = 0$. À cet effet, appliquons la Proposition 1 :

$$n \cdot \mathrm{PGCD}\left(a, \mathrm{ord}(z)\right) = \mathrm{ord}(z). \tag{3}$$

En particulier, $\mathrm{ord}(z)$ divise an. Puisque a et n sont premiers entre eux, on peut donc écrire $\mathrm{ord}(z) = dn'$ avec $d \mid a$ et $n' \mid n$. En injectant dans (3), on obtient $nd = dn'$. Donc $n = n'$, et $\mathrm{ord}(z) = dn$. Ainsi, z est racine primitive dn-ième avec $d \mid n$, ce qui conclut. □

Si p est un nombre premier et $k, n \geqslant 1$ sont des entiers, la Proposition 2 (iii) et une récurrence fournissent l'égalité

$$\Phi_{p^k n}(X) = \begin{cases} \Phi_n(X^{p^k}) & \text{si } p \mid n \\ \dfrac{\Phi_n(X^{p^k})}{\Phi_n(X^{p^{k-1}})} & \text{si } p \nmid n. \end{cases} \tag{4}$$

Pour calculer $\Phi_n(X)$, (4) nous permet de nous ramener au cas où n n'a pas de facteur carré.

Il est instructif d'utiliser les formules précédentes pour vérifier que

$$\Phi_1 = X - 1, \Phi_2 = X + 1, \Phi_3 = X^2 + X + 1, \Phi_4 = X^2 + 1, \Phi_5 = X^4 + X^3 + X^2 + X^2 + X^1, \Phi_6 = X^2 - X + 1,$$

que $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ si p est premier, et que $\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}}) = X^{(p-1)p^{k-1}} + \cdots + X^{p^{k-1}} + 1$.

Finalement, nous aurons besoin de minorer et majorer des polynômes cyclotomiques.

Lemme 3 (Encadrement des polynômes cyclotomiques)**.** *Soient $a \in \mathbb{C}$ et $n \geqslant 1$. On a*

$$\left||a| - 1\right|^{\phi(n)} \leqslant |\Phi_n(a)| \leqslant (|a| + 1)^{\phi(n)}.$$

De plus, lorsque $n > 2$, ces inégalités sont strictes.

Démonstration. En prenant le module dans la définition de $\Phi_n(a)$, on a

$$\Phi_n(a) = \prod_{z \text{ est racine primitive } n\text{-ième de l'unité}} |a - z|.$$

Le résultat découle alors de l'inégalité triangulaire. Lorsque $n > 2$, les racines primitives n-ièmes ne sont pas alignées avec 0, ce qui implique l'existence d'une racine primitive n-ième z telle que $\left||a| - 1\right| < |z - a| < |a| + 1$. □

5.4 Lien avec les propriétés d'ordre multiplicatif

Lemme 4. *Soient $a, n \geqslant 1$ des entiers et p un nombre premier. Supposons qu'il existe un polynôme $P \in \mathbb{Z}/p\mathbb{Z}[X]$ tel que l'égalité*

$$X^n - 1 = (X - a)^2 \cdot P(X)$$

ait lieu dans $\mathbb{Z}/p\mathbb{Z}[X]$. Alors p divise n.

Démonstration. On dérive l'égalité apparaissant dans l'énoncé du lemme :

$$nX^{n-1} = 2(X - a)P(X) + (X - a)^2 P'(X).$$

On évalue en $X = a$ pour obtenir que $na^{n-1} = 0$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Donc p divise na^{n-1}. Or 0 n'est pas racine de $X^n - 1$ dans $\mathbb{Z}/p\mathbb{Z}[X]$, donc p ne divise pas a. Donc p divise n. □

On en déduit le résultat suivant, concernant les diviseurs premiers de deux polynômes cyclotomiques évalués au même entier.

Lemme 5. *Soient $n \geqslant 1$ un entier et p un nombre premier. Soit d un diviseur de n avec $d \neq n$. On suppose que $p \mid \Phi_n(a)$ et que $p \mid \Phi_d(a)$. Alors p divise n.*

Démonstration. Comme p divise $\Phi_d(a)$, a est racine de Φ_d dans $\mathbb{Z}/p\mathbb{Z}[X]$. Donc il existe un polynôme $P_1 \in \mathbb{Z}/p\mathbb{Z}[X]$ tel que $\Phi_d(X) = (X - a)P_1(X)$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. De même, il existe un polynôme $P_2 \in \mathbb{Z}/p\mathbb{Z}[X]$ tel que $\Phi_n(X) = (X - a)P_2(X)$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. D'après le Théorème 6 (i), on a $X^n - 1 = (X - a)^2 R(X)$ dans $\mathbb{Z}/p\mathbb{Z}[X]$ pour un certain polynôme $R \in \mathbb{Z}/p\mathbb{Z}[X]$. Le Lemme 5 implique alors que p divise n. □

Ce lemme va nous permettre d'établir les deux théorèmes suivants concernant les polynômes cyclotomiques évalués en des entiers.

Théorème 7. *Soient $m, n \geqslant 1$ des entiers, $a \in \mathbb{Z}$ et p un nombre premier. On suppose que p divise $\Phi_m(a)$ et que p divise $\Phi_n(a)$. Alors il existe $k \in \mathbb{Z}$ tel que*

$$\frac{m}{n} = p^k.$$

De plus, $\mathrm{PGCD}\left(\Phi_m(a), \Phi_n(a)\right)$ *est une puissance de p.*

Démonstration. On écrit $m = p^\alpha M$ et $n = p^\beta N$ avec $p \nmid M$ et $p \nmid N$. On va montrer que $M = N$. Tout d'abord, $p \mid \Phi_m(a) \mid a^m - 1$, donc p ne divise pas a. Montrons que p divise $\Phi_M(a)$. On peut supposer $\alpha \geqslant 1$ (car sinon $m = M$ et il n'y a rien à faire). Alors, d'après la Proposition 2 (iii),

$$\Phi_m(a) = \frac{\Phi_M(a^{p^\alpha})}{\Phi_M(a^{p^{\alpha-1}})}.$$

Donc p divise $\Phi_M(a^{p^\alpha})$. Or $a^{p^\alpha} \equiv a \pmod{p}$ d'après le petit théorème de Fermat. Donc $0 \equiv \Phi_M(a^{p^\alpha}) \equiv \Phi_M(a) \pmod{p}$. On montre de même que p divise $\Phi_N(a)$.

Maintenant, raisonnons par l'absurde en supposant $M \neq N$. Sans perte de généralité, supposons que $M > N$ et posons $g = \mathrm{PGCD}\,(M, N)$. On a $p \mid \Phi_M(a) - 1 \mid a^M - 1$ et $p \mid \Phi_N(a) - 1 \mid a^N - 1$. Donc

$$p \mid \mathrm{PGCD}\left(a^M - 1, a^N - 1\right) \mid a^g - 1$$

d'après le Lemme 2. Le Corollaire 1 (ii) fournit alors l'existence d'un diviseur d de g tel que $p \mid \Phi_d(a)$. Or $p \mid \Phi_M(a)$ et on a $d \mid M, d \neq M$. D'après le Lemme 5, ceci implique que p divise M, ce qui est absurde. Le fait que $\mathrm{PGCD}\left(\Phi_m(a), \Phi_n(a)\right)$ soit une puissance de p est une conséquence immédiate de la première assertion. □

On peut remarquer que le Lemme 5 est un cas particulier du théorème 7.

Théorème 8. *Soit p un nombre premier, $n \geqslant 1$ et $a \in \mathbb{Z}$.*

(i) Si $p \mid \Phi_n(a)$, alors $p \equiv 1 \pmod{n}$ ou $p \mid n$.

(ii) Si $n = p^\alpha N$ avec p premier avec N et $p \mid \Phi_n(a)$, alors l'ordre de a modulo p vaut N.

(iii) Si p et n sont premiers entre eux, $p \mid \Phi_n(a)$ si, et seulement si, l'ordre de a modulo p vaut n.

Démonstration. Pour (i), on remarque d'abord que $p \mid \Phi_n(a) \mid a^n - 1$ et donc p ne divise pas a. Soit ω l'ordre de a modulo p. Comme $a^n \equiv 1 \pmod{p}$, ω divise n.

Premier cas : $\omega = n$. D'après le petit théorème de Fermat, $a^{p-1} \equiv 1 \pmod{p}$. On en déduit que $n = \omega \mid p-1$, de sorte que $p \equiv 1 \pmod{n}$.

Deuxième cas : $\omega < n$. Comme $p \mid a^\omega - 1$, le Corollaire 1 (ii) implique qu'il existe un diviseur d de ω tel que $p \mid \Phi_d(a)$. Or p divise $\Phi_n(a)$ et $d < n$ (car $d \leqslant \omega < n$). D'après le Lemme 5, p divise n.

Pour (ii), notons ω l'ordre de a modulo n. On a $1 \equiv a^n = (a^N)^{p^\alpha} \equiv a^N \pmod{p}$. Donc $\omega \mid N$. Si $\omega < N$, on raisonne comme dans la preuve de (i) : puisque $p \mid a^\omega - 1$, le Corollaire 1 (ii) implique qu'il existe un diviseur d de ω tel que $p \mid \Phi_d(a)$. Or $p \mid \Phi_n(a)$ et n/d n'est pas une puissance de p car $d \leqslant \omega < N$. Ceci contredit le Théorème 7, et donc $\omega = N$.

Pour (iii), le sens direct provient du deuxième point avec $\alpha = 0$. Pour la réciproque, supposons que l'ordre de a modulo p vaille n. Alors p divise $a^n - 1$, et d'après le Corollaire 1 (ii), il existe un diviseur d de n tel que $p \mid \Phi_d(a)$. D'après le sens direct, l'ordre de a modulo p vaut d. Donc $d = n$, ce qui conclut. □

Comme $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$, on en déduit le corollaire suivant.

Corollaire 2. *Soit $x \in \mathbb{Z}$. Si p, q sont deux nombres premiers tels que q divise $1 + x + \cdots + x^{p-1}$, alors $q \equiv 1 \pmod{p}$ ou $q = p$.*

5.5 Une application

Théorème 9 (Théorème de Dirichlet)**.** *Soit $n \geqslant 2$. Il existe une infinité de nombres premiers p tels que $p \equiv 1 \pmod{n}$.*

Démonstration. Par l'absurde, supposons qu'il n'en existe qu'un nombre fini. Notons T le produit de ces nombres, multiplié également par tous les diviseurs premiers de n. Comme $T > 1$, il existe un entier $k \geqslant 1$ tel que $\Phi_n(T^k) > 1$. Soit alors p un diviseur premier de $\Phi_n(T^k)$. D'après le Théorème 8 (i), ou bien $p \equiv 1 \pmod{n}$, ou bien p divise n. Or $p \mid \Phi_n(T^k) \mid T^{nk} - 1$, donc p est premier avec T. Donc p est premier avec n, ce qui implique $p \equiv 1 \pmod{n}$ et est absurde. □

5.6 Exercices

Exercice 21 Soit p un nombre premier. Montrer que $p^p - 1$ admet un diviseur premier congru à 1 modulo p.

Exercice 22 Soient $n, b \geqslant 2$ des entiers. Montrer que si $(b^n - 1)/(b - 1)$ est une puissance d'un nombre premier, alors n est une puissance d'un nombre premier (on verra à l'Exercice 40 qu'en fait n est un nombre premier).

Exercice 23 Soit $n \geqslant 1$ un entier. Prouver que $2^{2^n} + 2^{2^{n-1}} + 1$ est divisible par au moins n nombres premiers différents. Quel est le plus petit entier $n \geqslant 1$ tel que $2^{2^n} + 2^{2^{n-1}} + 1$ est divisible par au moins $n + 1$ nombres premiers différents ?

Exercice 24 (Liste courte Olympiades Internationales de Mathématiques 2002) Soit $n \geqslant 1$ un entier et soient $p_1, \ldots, p_n$ des nombres premiers impairs distincts. Montrer que $2^{p_1 p_2 \cdots p_n} + 1$ a au moins $2^{2^{n-1}}$ diviseurs.

Exercice 25 (Olympiades Iran 2013) Soit p un nombre premier et d un diviseur de $p - 1$. Trouver le produit de tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ dont l'ordre vaut d.

Exercice 26 (Liste courte Olympiades Internationales de Mathématiques 2006) Trouver tous les entiers relatifs x, y tels que $\dfrac{x^7 - 1}{x - 1} = y^5 - 1$.

Exercice 27 Prouver qu'il existe une infinité d'entiers positifs n tels que les diviseurs premiers de $n^2 + n + 1$ sont tous inférieurs ou égaux à $\sqrt{n}$.

6 Théorème de Zsigmondy

6.1 Un deuxième théorème de Zsigmondy

Tout d'abord, du Théorème 2 on peut aussi aisément déduire la version suivante :

Théorème 10 (Théorème de Zsigmondy bis)**.** *Soient $a > b \geqslant 1$ des entiers strictement positifs premiers entre eux et $n \geqslant 2$ un entier. Alors $a^n + b^n$ admet au moins un facteur premier qui ne divise pas $a^k + b^k$ pour tout $1 \leqslant k < n$, à l'exception du cas $2^3 + 1^3$.*

Démonstration. Supposons $(a, b, k) \neq (2, 1, 3)$. On peut alors appliquer le théorème de Zsigmondy à $a^{2n} - b^{2n}$: il existe un nombre premier p divisant $a^{2n} - b^{2n}$ mais pas $a^j - b^j$ lorsque $1 \leqslant j < 2n$. Donc p divise $(a^n - b^n)(a^n + b^n)$. Comme p ne divise pas $a^n - b^n$, il divise nécessairement $a^n + b^n$. Soit maintenant $1 \leqslant j < n$. Comme p ne divise pas $a^{2j} - b^{2j} = (a^j - b^j)(a^j + b^j)$, on en déduit que p ne divise pas $a^j + b^j$, ce qui conclut. □

Le reste de cette partie est consacré à la preuve du Théorème 2 en adaptant les références [1, 8, 9]. On fixe dans la suite $a > b \geqslant 1$ des entiers strictement positifs premiers entre eux et $n \geqslant 2$ un entier.

Prouvons déjà le théorème de Zsigmondy dans le cas $n = 2$, qui n'est pas difficile.

Preuve du Théorème 2 dans le cas $n = 2$. Supposons que $n = 2$ et que $a + b$ n'est pas une puissance de 2. Soit p un diviseur premier impair de $a+b$. Alors p ne divise pas $a-b$. En effet, si $p \mid a-b$, alors $p \mid a+b+(a-b) = 2a$ et $p \mid a+b-(a-b) = 2b$. Or a et b sont premiers entre eux, donc $p = 2$, ce qui contredit le fait que p soit impair. □

Dans la suite, on suppose $n > 2$ et on fixe des entiers $a > b \geqslant 1$ premiers entre eux.

6.2 Quelques propriétés des diviseurs premiers primitifs

Lemme 6. *Soit p un nombre premier divisant $a^n - b^n$. Alors p est non primitif si, et seulement si, il existe un diviseur d de n tel que $d < n$ et $p \mid a^d - b^d$.*

Démonstration. La réciproque est claire par définition, on se concentre donc sur l'implication. Soit p un diviseur premier non primitif de $a^k - b^k$ avec $k < n$. Soit $d = \mathrm{PGCD}\,(k, n)$. En particulier, $d \mid n$ et $d < n$. En utilisant le Lemme 2, on obtient $p \mid \mathrm{PGCD}\left(a^n - b^n, a^k - b^k\right) = a^d - b^d$. □

Lemme 7. *Soit p un nombre premier divisant $a^n - b^n$. Si p est primitif, alors $p \equiv 1 \pmod{n}$.*

Démonstration. Comme a et b sont premiers entre eux, p ne divise ni a, ni b. Il existe donc un entier c tel que $a \equiv bc \pmod{p}$. Alors, pour $j \geqslant 1$, $a^j - b^j \equiv b^j(c^j - 1) \pmod{p}$. Donc l'ordre de c modulo p vaut n. D'après le petit théorème de Fermat, $c^{p-1} \equiv 1 \pmod{p}$, et donc n divise $p - 1$. □

6.3 Idées de la preuve et résultats préliminaires

L'idée est d'introduire l'entier

$$\Psi_n = b^{\phi(n)} \Phi_n\left(\frac{a}{b}\right).$$

En effet, pour $b = 1$, le théorème de Zsigmondy implique l'existence d'un nombre premier p tel que l'ordre de a modulo p vaut n, et compte tenu du Théorème 8 (iii), il est naturel de considérer $\Phi_n(a)$.

L'identité clé est la suivante :

$$a^n - b^n = \prod_{d \mid n} \Psi_d. \tag{5}$$

Pour la prouver, on écrit, en utilisant le Théorème 6 (i) et le corollaire qui le suit,

$$\prod_{d \mid n} \Psi_d = \prod_{d \mid n} \left(b^{\phi(d)} \Phi_d\left(\frac{a}{b}\right)\right) = b^n \left(\left(\frac{a}{b}\right)^n - 1\right) = a^n - b^n.$$

Il en découle en particulier que $\Psi_n \mid a^n - b^n$ et que

$$\Psi_n = \prod_{d \mid n} \left(a^{\frac{n}{d}} - b^{\frac{n}{d}}\right)^{\mu(d)}. \tag{6}$$

en vertu du Théorème 5.

On utilisera aussi l'inégalité suivante :

$$(a - b)^{\phi(n)} < \Psi_n < (a + b)^{\phi(n)}, \tag{7}$$

avec inégalités strictes car $n > 2$. Cela se démontre exactement comme le Lemme 3 en remarquant que

$$\Psi_n = b^{\phi(n)} \prod_{z \text{ est racine primitive } n\text{-ième de l'unité}} \left(\frac{a}{b} - z\right) = \prod_{z \text{ est racine primitive } n\text{-ième de l'unité}} (a - bz).$$

Concluons cette partie par deux égalités utiles ultérieurement. Si p est un nombre premier divisant n, écrivons $n = p^\alpha N$ avec p ne divisant pas N. Posons $\Psi_n(x, y) = y^{\phi(n)}\Phi_n(x/y)$ pour des entiers $x, y \geqslant 1$ quelconques. Alors

$$\Psi_n(a, b) = \frac{\Psi_N\left(a^{p^\alpha}, b^{p^\alpha}\right)}{\Psi_N\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right)}, \qquad \Psi_n(a, b) = \Psi_{pN}\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right). \tag{8}$$

Cela se démontre aisément en utilisant (4) ; montrons par exemple la première égalité en utilisant le fait que $\phi(p^\alpha N) = \phi(p^\alpha)\phi(N) = p^{\alpha-1}(p-1)\phi(N)$:

$$\begin{aligned}
\Psi_n(a, b) &= b^{\phi(p^\alpha N)}\Phi_{p^\alpha N}\left(\frac{a}{b}\right) = b^{p^{\alpha-1}(p-1)\phi(N)} \frac{\Phi_N\left(a^{p^\alpha}/b^{p^\alpha}\right)}{\Phi_N\left(a^{p^{\alpha-1}}/b^{p^{\alpha-1}}\right)} \\
&= \frac{\left(b^{p^\alpha}\right)^{\phi(N)} \Phi_N\left(a^{p^\alpha}/b^{p^\alpha}\right)}{\left(b^{p^{\alpha-1}}\right)^{\phi(N)} \Phi_N\left(a^{p^{\alpha-1}}/b^{p^{\alpha-1}}\right)} \\
&= \frac{\Psi_N\left(a^{p^\alpha}, b^{p^\alpha}\right)}{\Psi_N\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right)}.
\end{aligned}$$

La deuxième égalité apparaissant dans (8) se démontre de la même manière. Pour simplifier, on écrira Ψ_n à la place de $\Psi_n(a, b)$.

6.4 Preuve du Théorème 2

Soit $a^n - b^n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la décomposition en facteurs premiers de $a^n - b^n$. Soient $p_{i_1}, \ldots, p_{i_j}$ les facteurs premiers primitifs de $a^n - b^n$. On pose alors

$$P_n = p_{i_1}^{\alpha_{i_1}} \cdots p_{i_j}^{\alpha_{i_j}},$$

qui est la "partie primitive" de $a^n - b^n$ (si $a^n - b^n$ n'a pas de facteurs premiers primitifs, on pose $P_n = 1$). Nous allons montrer que $P_n > 1$.

Étape 1. On montre que $P_n \mid \Psi_n$.

En effet, soit p un diviseur premier primitif de $a^n - b^n$. D'après le Lemme 6, si $d \mid n$ et $d \neq n$, alors p ne divise pas $a^d - b^d$, et donc p ne divise pas Ψ_d non plus d'après (5). On en déduit que p est premier avec $\prod_{d|n, d\neq n} \Psi_d$. Par (5), on en déduit que $v_p(a^n - b^n) = v_p(\Psi_n)$. Ceci étant vrai pour tout diviseur premier primitif de $a^n - b^n$, c'est-à-dire pour tout diviseur premier de P_n, cela implique que $P_n \mid \Psi_n$. □

Soit alors $\lambda \geqslant 1$ l'entier tel que

$$\Psi_n = \lambda \cdot P_n. \tag{9}$$

Tout d'abord, on remarque qu'on a bien $P_n > 1$ dans le cas $\lambda = 1$. En effet, d'après (7), on a $P_n = \Psi_n > (a-b)^{\phi(n)} \geqslant 1$. On suppose donc $\lambda > 1$ dans la suite.

Étape 2. Soit p un nombre premier qui divise λ. On montre que :

(i) Le nombre premier p n'est pas primitif. En particulier, $\mathrm{PGCD}(\lambda, P_n) = 1$.

(ii) On a $p \mid n$.

Pour (i), il suffit de remarquer que par définition de P_n, $\Psi_n/P_n = \lambda$ n'a pas de diviseurs premiers primitifs.

Prouvons (ii). Par (i), p n'est pas primitif, et d'après le Lemme 6, il existe $d_0 \neq n$ tel que $d_0 \mid n$ et $p \mid a^{d_0} - b^{d_0}$. Compte tenu de (5), on a

$$a^n - b^n = \Psi_n \cdot \left(a^{d_0} - b^{d_0}\right) \cdot \prod_{d|n, d\neq n, d\nmid d_0} \Psi_d.$$

Donc $p \mid \Psi_n \mid (a^n - b^n)/(a^{d_0} - b^{d_0})$.

Premier cas : $p \neq 2$. Dans ce cas, le théorème LTE donne

$$v_p(a^n - b^n) = v_p(a^{d_0} - b^{d_0}) + v_p(n/d_0).$$

Ainsi, si p ne divise pas n, alors $v_p(n/d_0) = 0$ et donc p ne divise pas $(a^n - b^n)/(a^{d_0} - b^{d_0})$, ce qui est absurde.

Deuxième cas : $p = 2$. Dans ce cas, $a^{d_0} - b^{d_0}$ est pair. Comme a et b sont premiers entre eux, cela entraîne que a et b sont impairs. Par l'absurde, supposons que n soit impair. Alors on peut écrire

$$a^n - b^n = \left(a^{d_0}\right)^{\frac{n}{d_0}} - \left(b^{d_0}\right)^{\frac{n}{d_0}} = (a^{d_0} - b^{d_0}) \cdot A,$$

où A est une somme de n/d_0 termes impairs. Donc A est impair et 2 ne divise pas $(a^n - b^n)/(a^{d_0} - b^{d_0})$, ce qui est absurde. □

Étape 3. On montre que λ est une puissance du plus grand nombre premier divisant n.

Soit p un nombre premier divisant λ. D'après l'étape 2, p divise n et on peut écrire $n = p^\alpha N$ avec p ne divisant pas N. Alors, par (8),

$$p \mid \Psi_n = \frac{\Psi_N\left(a^{p^\alpha}, b^{p^\alpha}\right)}{\Psi_N\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right)}.$$

Donc p divise $\Psi_N\left(a^{p^\alpha}, b^{p^\alpha}\right)$. Or, d'après le petit théorème de Fermat, $a^{p^\alpha} \equiv a \pmod p$ et $b^{p^\alpha} \equiv b \pmod p$, ce qui entraîne que

$$0 \equiv \Psi_N\left(a^{p^\alpha}, b^{p^\alpha}\right) \equiv \Psi_N(a, b) \pmod p.$$

Donc p divise Ψ_N. D'après l'étape 1 (appliquée avec N à la place de n), on peut écrire $\Psi_N = \lambda' \cdot P_N$, où P_N est la partie primitive de $a^N - b^N$ et λ' est un entier. Si p divise λ' alors p divise N d'après l'étape 2, ce qui n'est pas possible. Comme p divise Ψ_N, cela implique que p divise P_N. Donc p est un facteur premier primitif de $a^N - b^N$. Donc

$$p \equiv 1 \pmod N \tag{10}$$

par le Lemme 7. En particulier $p > N$. Ceci nous donne bien que p est bien le plus grand facteur premier de n, et donc que le seul diviseur premier de λ est p. □

Dans la suite, p désignera le plus grand diviseur premier de n et on écrit $n = p^\alpha N$ avec p ne divisant pas N.

Étape 4. On montre que $\lambda = p$.

Pour cela, comme $\Psi_n = \lambda \cdot P_n$ et que PGCD $(\lambda, P_n) = 1$ (d'après l'étape 2), il suffit de montrer que $v_p(\Psi_n) = 1$.

Considérons un entier $d \geqslant 1$ tel que $d \mid n$ et $p \mid a^d - b^d$. En particulier, comme a et b sont premiers entre eux, p ne divise pas b. Soit c un entier tel que $bc \equiv 1 \pmod p$. Nous avons déjà vu que p divise Ψ_n. Ainsi

$$0 \equiv \Psi_n = b^{\phi(n)} \Phi_n\left(\frac{a}{b}\right) \equiv b^{\phi(n)} \Phi_n(ac) \pmod p.$$

Donc $p \mid \Phi_n(ac)$. Le Théorème 8 (ii) entraîne que l'ordre de ac modulo p vaut N. Or $p \mid a^n - b^n$ (car $a^d - b^d \mid a^n - b^n$). Donc $(ac)^d \equiv 1 \pmod p$ et N divise d.

Intéressons nous maintenant aux termes divisibles par p dans le produit (6). Compte tenu de ce qui précède, si $d \mid n$ et si p divise $a^{\frac{n}{d}} - b^{\frac{n}{d}}$, alors $N \mid n/d$, ce qui implique que $d = p^i$ pour un certain entier $i \geqslant 0$. Comme $\mu(p^i) = 0$ dès que $i \geqslant 2$, la factorisation (6) entraîne que

$$v_p(\Psi_n) = v_p\left(\frac{a^n - b^n}{a^{\frac{n}{p}} - b^{\frac{n}{p}}}\right).$$

Premier cas : $p \neq 2$. Alors le théorème LTE donne immédiatement $v_p(\Psi_n) = 1$.

Deuxième cas : $p = 2$. Nous avons déjà établi qu'alors a et b sont impairs, et que p est le plus grand diviseur premier de n. Donc n est une puissance de 2. Comme $n > 2$, écrivons $n = 2^k$ avec $k \geqslant 2$. Mais alors

$$\frac{a^n - b^n}{a^{\frac{n}{p}} - b^{\frac{n}{p}}} = \frac{a^{2^k} - b^{2^k}}{a^{2^{k-1}} - b^{2^{k-1}}} = a^{2^{k-1}} + b^{2^{k-1}} \equiv 2 \pmod 4.$$

Ainsi $v_2(\Psi_n) = 1$. □

Étape 5. Étude du cas $\lambda = p$: fin de la preuve du théorème.
Tout d'abord, si $a - b \geqslant 2$, alors en utilisant successivement (9) et (7), on a

$$P_n = \frac{1}{p}\Psi_n > \frac{1}{p}(a-b)^{\phi(n)} \geqslant \frac{2^{\phi(n)}}{p} = \frac{2^{p^{\alpha-1}(p-1)\phi(N)}}{p} \geqslant \frac{2^{p-1}}{p} \geqslant 1,$$

et donc $P_n > 1$ dans ce cas.

Supposons donc $a - b = 1$. Raisonnons par l'absurde en supposant $P_n = 1$. Alors $\Psi_n = p$. De plus, comme p divise $(b+1)^n - b^n$, p est impair.

Premier cas : $\alpha > 1$. En vertu de successivement (8) et (7), on a

$$p = \Psi_N = \Psi_{pN}\left((b+1)^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right) > \left((b+1)^{p^{\alpha-1}} - b^{p^{\alpha-1}}\right)^{\phi(pN)} \geqslant (b+1)^p - b^p = \sum_{i=0}^{p-1}\binom{p}{i}b^i > p,$$

ce qui est absurde.

Deuxième cas : $\alpha = 1$. On remarque d'abord que $a^p - b^p \geqslant a + b$ car $a^p - b^p = \displaystyle\sum_{i=0}^{p-1}\binom{p}{i}b^i \geqslant pb + 1 \geqslant 2b + 1$.
Alors, en vertu de (8) et (7), on a

$$p = \Psi_N = \frac{\Psi_N\left(a^p, b^p\right)}{\Psi_N} > \left(\frac{a^p - b^p}{a+b}\right)^{\phi(N)} \geqslant \frac{a^p - b^p}{a+b} = \frac{1}{2b+1}\sum_{k=0}^{p-1}\binom{p}{k}b^k \geqslant \frac{b}{2b+1}\sum_{k=1}^{p-1}\binom{p}{k}$$

Or $b/(2b+1) \geqslant 1/3$ pour tout entier $b \geqslant 1$ et $\displaystyle\sum_{k=1}^{p-1}\binom{p}{k} = 2^p - 2$. Ainsi, $3p > 2^p - 2$, ce qui force $p = 3$.

La congruence (10) entraîne que N divise 2. Ainsi, $n = 3$ ou $n = 6$. Traitons d'abord le cas $n = 3$. On a

$$3 = \Psi_3 = b^2\left(1 + \frac{a}{b} + \frac{a^2}{b^2}\right) = a^2 + ab + b^2 = 1 + 3b + 3b^2,$$

ce qui est impossible. Finalement, si $n = 6$, on a

$$3 = \Psi_6 = b^2\left(1 - \frac{a}{b} + \frac{a^2}{b^2}\right) = a^2 - ab + b^2 = 1 + b + b^2.$$

Ceci entraîne $b = 1$ et $a = 2$, qui est précisément la dernière exception du théorème de Zsigmondy. Ceci conclut (enfin !) la preuve de ce théorème.

Remarque 1. *Dans la preuve précédente, nous avons en particulier établi qu'en toute généralité, on a soit $\Psi_n = P_n$, soit $\Psi_n = p \cdot P_n$, où p est le plus grand diviseur premier de n.*

6.5 Exercices

Exercice 28 Pour un entier $n \geqslant 2$, notons a_n le nombre entier dont l'écriture décimale comporte n fois le chiffre 1. Soit $n \geqslant 1$. Existe-t-il un nombre premier p divisant a_n mais pas $a_{n-1}, \ldots, a_1$?

Exercice 29 (Olympiades Italie 2003) Trouver tous les entiers strictement positifs (a, b, p) avec p premier tels que $2^a + p^b = 19^a$.

Exercice 30 (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 31 (Olympiades Iran) Soit A un ensemble fini de nombres premiers et soit $a \geqslant 2$ 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 32 (D'après liste courte Olympiades Internationales de Mathématiques 2002) Soit $n \geqslant 1$ 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 33 (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 34 (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 35 (Compétition Tchéco-Slovaque 1996) Trouver tous les entiers strictement positifs x, y, p tels que $p^x - y^p = 1$ avec p premier.

Exercice 36 (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 37 (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 38 (Olympiades Balkaniques de Mathématiques 2009) Trouver tous les entiers strictement positifs x, y, z tels que $5^x - 3^y = z^2$.

Exercice 39 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 40 (Olympiade Estonie 2007) Soient $n, b \geqslant 2$ des entiers. Montrer que si $(b^n - 1)/(b-1)$ est une puissance d'un nombre premier, alors n est un nombre premier.

Exercice 41 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 42 (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 43 (Olympiade Angleterre 1996) Trouver les entiers positifs x, y, z tels que $2^x + 3^y = z^2$.

Exercice 44 Résoudre l'exercice 4 en vous aidant du théorème de Zsigmondy.

Exercice 45 Résoudre l'exercice 19 en vous aidant du théorème de Zsigmondy.

Exercice 46 (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 47 (Olympiade Iran 2006) Soient $a, b, c, k \geqslant 1$ 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.

Exercice 48 Existe-t-il une infinité de couples (p, q) de nombres premiers tels que $pq \mid 2^{p-1} + 2^{q-1} - 2$?

Exercice 49 Soit p un nombre premier. Si $m \geqslant 1$ est un entier, on pose $|m|_p = p^k$ si $p^k \mid m$ et $p^{k+1} \nmid m$.

(i) (Théorème de Feit) Soit $N > 1$ fixé. Alors pour tous les couples d'entiers (a, n) avec $a > 1$ et $n > 2$, sauf éventuellement pour un nombre fini d'entre eux, il existe un diviseur premier primitif p de $a^n - 1$ tel que $|a^n - 1|_p > nN + 1$.

(ii) Si $m \geqslant 1$ est un entier, on note maintenant $[m]_p$ le plus grand diviseur de m qui n'est pas divisible par p. Montrer que si p est un nombre premier et que si $a \geqslant 2$ est un entier, alors

$$\frac{[a^n - 1]_p}{n} \underset{n\to\infty}{\longrightarrow} \infty.$$

7 Solutions des exercices

Solution de l'exercice 1 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 $v_p(a-1) \geqslant n-1$, ce qu'il fallait démontrer.

Solution de l'exercice 2 Soit $k \geqslant 1$ 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 $v_3(4-1)+v_3(n) = v_3(4^n-1) \geqslant k$. On en déduit que $v_3(n) \geqslant k-1$. 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.

Solution de l'exercice 3 Par convexité de $x \mapsto x^p$, on a $(x^p+y^p)/2 \geqslant ((x+y)/2)^p$. Par hypothèse, il s'ensuit que $m \geqslant p$. Soit $d = \mathrm{PGCD}(x,y)$, $x = dX$, $y = dY$. L'équation se réécrit

$$2^{m-1}(X^p+Y^p) = d^{m-p}(X+Y)^m. \tag{11}$$

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 $v_q(d^{m-p}(X+Y)^m) \geqslant mv_q(X+Y)$. Donc $v_q(X+Y)+v_q(p) \geqslant mv_q(X+Y)$. Ceci implique $m \leqslant 2$, et donc $m = p = 2$ car $m \geqslant p$, 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 $v_2(X+Y) \leqslant v_2(X^p+Y^p)$. À présent, en prenant la valuation 2-adique dans l'égalité (11), on obtient $m-1+v_2(X+Y) \geqslant mv_2(X+Y)$. Ainsi $v_2(X+Y) \leqslant 1$, $X+Y \leqslant 2$, et donc $X = Y = 1$ et $m = p$.

Solution de l'exercice 4 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 $x^{2008}-x^{2007}y \geqslant 1, x^{2006}y^2-x^{2005}y^3 \geqslant 1$ et ainsi de suite, de sorte que la somme totale sera au moins égale à 1004. Il n'y a donc pas de solutions.

Solution de l'exercice 5 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.

Solution de l'exercice 6 Soit $n \geqslant 1$ tel que 9 divise 7^n+n^3. Comme un cube est congru à $0, -1$ ou 1 modulo 9, on en déduit que $n^6 \equiv 1 \bmod 9$ et donc que $7^{2n} \equiv 1 \pmod 9$. Or l'ordre de 7 modulo 9 est 3. On en déduit que 3 divise $2n$. Ainsi 3 divise n. Il faudrait donc que 3 divise 7^n, ce qui est absurde. Il n'y a donc pas de tels entiers.

Solution de l'exercice 7 On suppose $m, n \geqslant 2$. Soit p le plus petit diviseur de n. Alors $3^{2n} \equiv 1 \bmod p$. Soit ω l'ordre de 3 modulo p. Alors ω divise $2n$. D'autre part, d'après le petit théorème de Fermat, $3^{p-1} \equiv 1 \pmod p$. Ainsi ω divise $p-1$. On en déduit que ω divise $\mathrm{PGCD}(p-1, 2n)$. D'après la condition sur p, on a nécessairement $\omega = 1$ ou 2. Dans le premier cas, $3 \equiv 1 \pmod p$ et donc $p = 2$. Dans le deuxième cas, $3^2 \equiv 1 \pmod p$ et donc $p = 2$. On en déduit que n est pair. On montre de même que m est pair. Alors 4 divise 3^m+1, ce qui n'est pas possible car m est pair.

Il reste à examiner le cas où m ou n vaut 1 et il vient que les solutions sont $(1,1)$, $(1,2)$ et $(2,1)$.

Solution de l'exercice 8 Il est clair que $q \geqslant 5$. Notons ω l'ordre 3/2 modulo q (ici, et similairement dans la suite, 1/2 désigne l'inverse de 2 modulo q). Alors ω divise p, donc $\omega = 1$ ou p. Le premier cas n'étant pas possible, on a donc $\omega = p$. Or d'après le petit théorème de Fermat, $(3/2)^{q-1} \equiv 1 \pmod q$. On en tire que ω divise $q-1$, d'où le résultat.

Solution de l'exercice 9 Supposons que $n \geqslant 2$. Soit p le plus petit facteur premier de n. Alors p divise $(a+1)^n - a^n$. En d'autres termes, $((a+1)/a)^n \equiv 1 \pmod{p}$. Soit ω l'ordre de $(a+1)/a$ modulo p. Alors ω divise n. D'autre part, d'après le petit théorème de Fermat, $((a+1)/a)^{p-1} \equiv 1 \pmod{p}$ de sorte que ω divise $p-1$. D'après la condition sur p, nécessairement $\omega = 1$. Ceci implique $a+1 \equiv a \pmod{p}$, ce qui est absurde.

Les solutions sont donc $n = 1$ et a quelconque.

Solution de l'exercice 10 Raisonnons par l'absurde et considérons un entier $k > 1$ tel que k^2 divise $a^k + b^k$. En raisonnant modulo 4 on voit que k est impair. Comme $a+b$ est une puissance de 2, il en découle que a et b sont premiers entre eux. Soit p le plus petit facteur premier de k qui est donc différent de 2 et ne divise ni a, ni b.

Soit ω l'ordre de $-a/b$ modulo p. Comme $a^k + b^k \equiv 0 \pmod{p}$, on a $(a/b)^k \equiv -1 \pmod{p}$, soit, puisque k est impair, $(-a/b)^k \equiv 1 \pmod{p}$. Ainsi, ω divise k, mais aussi $p-1$ d'après le petit théorème de Fermat. Par définition de p, k et $p-1$ sont premiers entre eux. Donc $\omega = 1$. Ainsi, $a + b \equiv 0 \pmod{p}$, ce qui est absurde et conclut la solution.

Solution de l'exercice 11 Les conditions de l'énoncé impliquent que $9^n \equiv 8^n \pmod{19}$. Mais l'inverse de 8 modulo 19 est 12. On en déduit que $13^n \equiv 108^n \equiv (9 \times 8)^n \equiv 1 \pmod{19}$. Or 13 est racine primitive modulo 19. Les entiers recherchés sont donc les multiples de 18.

Solution de l'exercice 12 Traitons d'abord le cas où a et b sont premiers entre eux. Alors a et b sont premiers avec $a^n - b^n$ et il est clair que l'ordre de a/b modulo $a^n - b^n$ est n. On en déduit que n divise $\phi(a^n - b^n)$.

Si $d > 1$ est le PGCD de a et de b, notons $u = a/d$ et $v = b/d$ de sorte que u et v sont premiers entre eux. D'après ce qui précède, n divise $\phi(u^n - v^n)$. En utilisant la formule exprimant $\phi(N)$ en fonction des facteurs premiers de N, on voit que $\phi(u^n - v^n)$ divise $\phi(d^n(u^n - v^n)) = \phi(a^n - b^n)$, ce qui conclut.

Solution de l'exercice 13 Soit p le plus petit facteur premier de n. Modulo p, l'ordre de k divise n puisque $k^n \equiv 1 \pmod{p}$. Par ailleurs, d'après le théorème de Fermat, l'ordre de k modulo p divise $p-1$. Or p est le plus petit facteur premier de n : le seul diviseur de n strictement inférieur à p est 1. L'ordre de p, diviseur de n inférieur ou égal à $p-1$, vaut donc nécessairement 1, ce qui prouve précisément que $k \equiv 1 \pmod{p}$, donc que p divise $k-1$, de sorte que $\mathrm{PGCD}(n, k-1)$ vaut au moins p. La réponse est donc non.

Solution de l'exercice 14 k n'est pas supposé premier, mais si tous ses facteurs premiers vérifient le résultat, alors un produit de nombres congrus à 1 $\pmod{2^{n+1}}$ sera lui-même $\equiv 1 \pmod{2^{n+1}}$. Il suffit donc de démontrer que tout facteur premier p de $x^{2^n} + y^{2^n}$ vérifie $p \equiv 1 \pmod{2^{n+1}}$. Par ailleurs, si p divisait x, comme par hypothèse il divise $x^{2^n} + y^{2^n}$, il diviserait également y : x et y ne seraient pas premiers entre eux. Donc x et p sont premiers entre eux, et y et p sont premiers entre eux. Notons $1/x$ l'inverse de x modulo p, de sorte que $x^{2^n} + y^{2^n} \equiv x^{2^n}\left(1 + (y/x)^{2^n}\right) \equiv 0 \pmod{p}$ équivaut à : $(y/x)^{2^n} \equiv -1 \pmod{p}$. Donc cet élément y/x a pour ordre 2^{n+1}, car 2^{n+1} est la première puissance de 2 vérifiant $(y/x)^{2^k} \equiv 1 \pmod{p}$, et 2^{n+1} n'a pas d'autre diviseur que des puissances de 2. Comme $(y/x)^{p-1} \equiv 1 \pmod{p}$, 2^{n+1} divise $p-1$, ce qui est précisément le résultat cherché. Un cas particulier important : pour $n = 1$, tout diviseur d'une somme de deux carrés premiers entre eux est congru à 1 modulo 4.

Solution de l'exercice 15 Remarquons tout d'abord que si $p = 2$, $2q$ divise $4+2^q$ si et seulement si soit $q = 2$, soit $2q$ divise 6, puisque pour tout q impair q divise $2^{q-1}-1$, donc $2q$ divise $2^q - 2$. D'où les solutions : $(p, q) = (2, 2), (2, 3)$ ou $(3, 2)$. On supposera désormais p et q impairs. Appelons ω_p et ω_q les ordres de 2 modulo p et q respectivement. Si p divise $2^p + 2^q$, donc $2^{p-1} + 2^{q-1}$, comme p divise $2^{p-1} - 1$, p divise $2^{q-1} + 1$, donc $2^{2(q-1)} - 1$. Dès lors, ω_p divise $p-1$ et $2(q-1)$ mais ne divise pas $q-1$. Si la plus grande puissance de 2 divisant ω_p (resp ω_q) est 2^{v_p} (resp 2^{v_q}), le fait que ω_p divise $2(q-1)$ et pas $q-1$ entraîne que $v_p > v_q$, car $q-1$ est divisible par ω_q donc par 2^{v_q} et pas par 2^{v_p}. Le même raisonnement, en échangeant p et q, aboutit à $v_q > v_p$, ce qui est manifestement incompatible. Il n'existe donc pas de couples de nombres premiers impairs vérifiant cette condition.

Solution de l'exercice 16 Si $p = 2$, $2^2 + 3^2 = 13$ vérifie bien la relation demandée : ce n'est pas une puissance $\geqslant 2$ d'un entier. Si maintenant p est impair, $2^p + 3^p$ est divisible par $2 + 3 = 5$, et n'est divisible par 25 que si p est divisible par 5 donc, puisque par hypothèse p est premier, si $p = 5$. En effet, $3^p = (5-2)^p \equiv (-2)^p + p.5(-2)^{p-1} \pmod{25}$. C'est aussi une conséquence du théorème LTE. On en déduit que, hormis éventuellement pour $p = 5$, le facteur 5 apparaît avec l'exposant 1, ce qui suffit à démontrer le résultat cherché. Pour $p = 5$, il apparaît bien avec l'exposant 2, mais $3^5 + 2^5 = 275$ n'est pas une puissance $\geqslant 2$ d'un entier, ce qui achève la démonstration.

Solution de l'exercice 17 C'est une conséquence presque immédiate de l'exercice 14. Soit 2^k la plus grande puissance de 2 divisant $n-1$: posons $n - 1 = 2^k q$, $s = m^{n-1} + 1 = x^{2^k} + y^{2^k}$ avec $x = m^q$ et $y = 1$. D'après l'exercice

14, tout diviseur de s est donc congru à 1 modulo 2^{k+1}. Or par définition de 2^k, n n'est pas congru à 1 modulo 2^{k+1}. Donc n ne divise pas s.

Solution de l'exercice 18 Les nombres entiers 1 et 3 sont solutions. Montrons qu'il n'y en a pas d'autres. Il est clair que n est impair. Ensuite, en considérant p le plus petit facteur premier de n et ω, l'ordre de 2 modulo p, on voit que ω divise à la fois $2n$ et $p-1$. Par définition de p, le PGCD de ces deux entiers vaut 2. Donc $2^2 \equiv 1 \pmod{p}$. Donc $p = 3$. Écrivons $n = 3u$, avec $u \geqslant 2$ et appliquons le théorème LTE (n est impair) : $2v_3(n) \leqslant v_3(2^n+1) = v_3(2+1)+v_3(n) = 1+v_3(n)$. Donc $v_3(n) = 1$ et 3 ne divise pas u. Soit maintenant q le plus petit diviseur premier de u. Alors $q \mid 8^u+1$. Donc, en notant ω' l'ordre de 8 modulo q, comme précédemment, ω' divise le PGCD de $2u$ et $q-1$, qui vaut 2. Donc q divise 63, soit $q = 7$. Finalement, écrivons $n = 21r$, avec $r \geqslant 1$. Alors $7 \mid 2^{21r}+1 \equiv 2 \pmod{7}$, ce qui est absurde.

Solution de l'exercice 19 On suppose $n > 2$ et que $3^n - 2^n = p^k$ pour $k \geqslant 1$. Montrons d'abord que n est impair. Si $n = 2n'$, alors $3^n - 2^n = (3^{n'}-2^{n'})(3^{n'}+2^{n'})$. Il existe donc $\alpha > \beta \geqslant 0$ tels que : $3^{n'}+2^{n'} = p^\alpha$ et $3^{n'}-2^{n'} = p^\beta$. Alors $2^{n'+1} = p^\beta(p^{\alpha-\beta}-1)$. Donc $p = 2$, ce qui est absurde, ou $\beta = 0$ qui conduit à $n = 2$, exclu. Ainsi n est impair.

Raisonnons par l'absurde et considérons q est un nombre premier divisant n avec $q < n$. Écrivons $n = qr$. Un raisonnement direct montre que $3^q - 2^q$ est une puissance de p, disons $3^q - 2^q = p^{k'}$ avec $k' < k$. En appliquant LTE, on voit que $v_p(r) = k - k'$. Écrivons donc $r = p^{k-k'}u$ avec p ne divisant pas u. Alors :

$$\begin{aligned} p^k &= 3^n - 2^n = 3^{qp^{k-k'}u} - 2^{qp^{k-k'}u} = (3^q)^{p^{k-k'}u} - (2^q)^{p^{k-k'}u} \\ &= (p^{k'}+2^q)^{p^{k-k'}u} - (2^q)^{p^{k-k'}u} \geqslant p^{k-k'}u \cdot p^{k'} \cdot 2^{q(p^{k-k'}u-1)} = p^k u \cdot 2^{q(p^{k-k'}u-1)} > p^k, \end{aligned}$$

ce qui est absurde : n est donc premier.

Solution de l'exercice 20 On commence par examiner la condition « p divise $1+q^r$ ». Elle se récrit $q^r \equiv -1 \pmod{p}$ et implique donc, en particulier, $q^{2r} \equiv 1 \pmod{p}$. Ainsi l'ordre de q modulo p est un diviseur de $2r$. Comme r est supposé premier, c'est donc un élément de l'ensemble $\{1, 2, r, 2r\}$. Si on suppose en outre que $p \neq 2$, on a $q^r \neq 1 \pmod{p}$, et donc l'ordre de q modulo p est nécessairement 2 ou $2r$. Dans le premier cas, en utilisant que p est premier, on obtient $q \equiv -1 \pmod{p}$, alors que dans le deuxième cas, on en déduit que $2r$ divise $p-1$. En permutant les nombres p, q et r, on obtient bien sûr des conséquences analogues des deux autres conditions « q divise $1+r^p$ » et « r divise $1+p^q$ ».

On suppose maintenant que p, q et r sont tous les trois impairs, et pour commencer que l'on est dans le cas où $q \equiv -1 \pmod{p}$. Le nombre premier p ne peut donc pas diviser $q-1$ (puisqu'il divise déjà $q+1$ et qu'il ne vaut pas 2). D'après les résultats du premier alinéa, la condition « q divise $1+r^p$ » implique donc que $r \equiv -1 \pmod{q}$. En appliquant à nouveau le même argument, on trouve que $p \equiv -1 \pmod{r}$. Or les trois congruences précédentes ne sont pas compatibles. En effet, par exemple, elles impliquent $q \geqslant p-1$, $r \geqslant q-1$ et $p \geqslant r-1$, ce qui ne peut se produire, étant donné que p, q et r sont des nombres premiers impairs, que si $p = q = r$; on a alors manifestement $q \not\equiv -1 \pmod{p}$. On en déduit que, toujours dans le cas où p, q et r sont supposés impairs, $2r$ divise $p-1$. En permutant circulairement les variables, on démontre de même que $2p$ divise $q-1$ et $2q$ divise $r-1$. Ainsi $8pqr$ divise $(p-1)(q-1)(r-1)$, ce qui n'est pas possible étant donné que $8pqr > (p-1)(q-1)(r-1)$. Finalement, il n'y a pas de solution lorsque p, q et r sont tous les trois impairs.

On en vient à présent au cas où l'un de ces trois nombres est égal à 2. Quitte à permuter circulairement à nouveau p, q et r, on peut supposer que c'est p. Les conditions de l'énoncé disent alors que q est impair, que $r^2 \equiv -1 \pmod{q}$ et que $2^q \equiv -1 \pmod{r}$. Selon ce qui a été fait dans le premier alinéa, cette dernière congruence entraîne que $r = 3$ ou que $2q$ divise $r-1$. Le premier cas conduit à $9 \equiv -1 \pmod{q}$, ce qui ne se produit que si $q = 5$ puisque l'on a déjà écarté le cas $q = 2$. On vérifie par ailleurs que le triplet $(2, 5, 3)$ est bien solution. Dans le second cas, le produit $2q$ divise $r-1$, mais aussi $2(r^2+1)$ puisqu'on sait que $r^2 \equiv -1 \pmod{q}$. Ainsi $2q$ divise $2(r^2+1) - 2(r+1)(r-1) = 4$, ce qui ne peut arriver.

En conclusion, il y a exactement trois solutions qui sont les triplets $(2, 5, 3)$, $(5, 3, 2)$ et $(3, 2, 5)$.

Solution de l'exercice 21 Soit q un diviseur premier de $(p^p-1)/(p-1) = \Phi_p(p)$. D'après le Corollaire 2, on a $q = p$ ou $q \equiv 1 \pmod{p}$. Le premier cas étant exclu car q divise p^p-1, le résultat demandé en découle.

Solution de l'exercice 22 Écrivons

$$\frac{b^n-1}{b-1} = \prod_{d \mid n, d \neq 1} \Phi_d(b) = \prod_{d \mid n, d \neq 1} |\Phi_d(b)|.$$

Ainsi, pour tout diviseur $d \mid n$, $d \neq 1$, $|\Phi_d(b)|$ est une puissance de p. D'après le Théorème 7, cela implique que pour tous diviseurs $d, d' \mid n$, $d, d' \neq 1$, d/d' est de la forme p^k avec $k \in \mathbb{Z}$. On en déduit que n est une puissance de p.

Solution de l'exercice 23 On commence par remarquer que

$$2^{2^n} + 2^{2^{n-1}} + 1 = \Phi_3\left(2^{2^{n-1}}\right) = \prod_{d \mid 2^{n-1}} \Phi_{3d}(2).$$

D'après le lemme 3, on a $\Phi_{3d}(2) > 1$. Il suffit de vérifier que si d et d' sont deux diviseurs distincts de 2^{n-1}, alors $\Phi_{3d}(2)$ et $\Phi_{3d'}(2)$ sont premiers entre eux. Supposons par l'absurde que ce ne soit pas le cas et choisissons un nombre premier p qui divise leur PGCD. D'après le Théorème 7, d/d' est une puissance de p, donc $p = 2$. Or $2^{2^n} + 2^{2^{n-1}} + 1$ est impair, ce qui implique que 2 ne divise pas $\Phi_{3d}(2)$.

D'après ce qui précède, le plus petit entier $n_0 \geqslant 1$ tel que $2^{2^{n_0}} + 2^{2^{n_0-1}} + 1$ est divisible par au moins $n_0 + 1$ nombres premiers différents est le plus petit entier $n_0 \geqslant 1$ tel que $\Phi_{3\cdot 2^{n_0-1}}(2)$ n'est pas un nombre premier. Comme $\Phi_3(x) = 1 + x + x^2$ et $\Phi_{3\cdot 2^{n_0-1}}(x) = 1 - x^{2^{n_0-2}} + x^{2^{n_0-1}}$ pour $n_0 \geqslant 2$, on vérifie que $\Phi_3(2) = 7$, $\Phi_{3\cdot 2}(2) = 3$, $\Phi_{3\cdot 2^2}(2) = 13$, $\Phi_{3\cdot 2^3}(2) = 241$ sont premiers, mais que $\Phi_{3\cdot 2^4}(2) = 65281 = 97 \cdot 673$ ne l'est pas, de sorte que $n_0 = 5$.

Solution de l'exercice 24 On va montrer que $2^{p_1 p_2 \cdots p_n} + 1$ a au moins 2^{n-1} diviseurs premiers distincts, ce qui conclura. D'après la Proposition 2 (i), on a

$$2^{p_1 p_2 \cdots + p_n} + 1 = \prod_{d \mid p_1 \cdots p_n} \Phi_{2d}(2).$$

D'après le Théorème 7, si $\Phi_{2d}(2)$ et $\Phi_{2d'}(2)$ ne sont pas premiers entre eux, alors d/d' est une puissance d'un nombre premier. De plus, d'après le Lemme 3 on a $\Phi_{2d}(2) > 1$ pour $d > 1$ et on vérifie que $\Phi_2(2) > 1$. Il suffit donc de trouver une collection de 2^{n-1} diviseurs de $p_1 \cdots p_n$ tels que le quotient de deux quelconques d'entre eux n'est pas une puissance d'un nombre premier. Pour cela, il suffit de choisir les diviseurs de $p_1 \cdots p_n$ qui ont un nombre pair de facteurs premiers : il y en a exactement 2^{n-1}.

Solution de l'exercice 25 D'après le Théorème 8 (iii), le problème revient à calculer le produit des éléments $a \in \mathbb{Z}/p\mathbb{Z}$ tels que $\phi_d(a) = 0$ dans $\mathbb{Z}/p\mathbb{Z}$, qui vaut, d'après les relations de Viète, $(-1)^{\phi(d)}\Phi_d(0)$ dans $\mathbb{Z}/p\mathbb{Z}$. Pour $d = 2$, cette dernière quantité vaut -1. Pour $d > 2$, celle ci vaut 1 car $\phi(d)$ est pair et $\Phi_d(0) = 1$ car les racines de Φ_d, de module 1, peuvent être réparties en couples de racines conjuguées.

Solution de l'exercice 26 L'égalité est équivalente à $1 + x + \cdots + x^6 = (y-1)(1 + y + y^2 + y^3 + y^4)$. Comme $1 + x + \cdots + x^6 = \Phi_7(x)$, d'après le Corollaire 2, un diviseur premier de $1 + x + \cdots + x^6$ est soit égal à 7, soit est congru à 1 modulo 7. Ainsi, un diviseur de $1 + x + \cdots + x^6$ est soit divisible par 7, soit congru à 1 modulo 7.

Ainsi, $y \equiv 1 \pmod 7$ ou $y \equiv 2 \pmod 7$. Dans le premier cas, $1 + y + y^2 + y^3 + y^4 \equiv 5 \pmod 7$, ce qui n'est pas possible, alors que dans le second cas, on a $1 + y + y^2 + y^3 + y^4 \equiv 2 \pmod 7$, ce qui n'est pas possible non plus. Il n'y a donc pas de solutions.

Solution de l'exercice 27 On remarque que $n^2 + n + 1 = \Phi_3(n)$. Afin de factoriser cette expression, l'idée est de considérer des entiers n de la forme $n = k^m$ avec m un entier fixé non divisible par 3 défini ultérieurement. En effet, dans ce cas, d'après la Proposition 2 (v),

$$n^2 + n + 1 = \Phi_3(k^m) = \prod_{d \mid m} \Phi_{3d}(k).$$

Si pour tout diviseur d de m on a $\Phi_{3d}(k) < \sqrt{n} = k^{m/2}$, c'est gagné. Or en vertu du Lemme 3, on a

$$\Phi_{3d}(k) < (k+1)^{\phi(3d)} \leqslant (k+1)^{\phi(3m)} = (k+1)^{2\phi(m)}.$$

Choisissons pour m un entier tel que $\phi(m)/m < 1/10$. Ceci est possible. En effet, si on note $(p_n)_{n \geqslant 1}$ la suite croissante des nombres premiers à partir de $p_1 = 5$, il est connu que la somme $\displaystyle\sum_{i \geqslant 1} \frac{1}{p_i}$ est infinie. Ainsi, si on pose $m_k = p_1 p_2 \cdots p_k$ pour tout $k \geqslant 1$, alors

$$\ln\left(\frac{\phi(m_k)}{m_k}\right) = \sum_{i=1}^{k} \ln\left(1 - \frac{1}{p}\right) \leqslant -\sum_{i=1}^{k} \frac{1}{p_i}.$$

Ainsi, $\ln(\phi(m_k)/m_k) \to -\infty$ lorsque $k \to \infty$, ce qui implique que $\phi(m_k)/m_k \to 0$ lorsque $k \to \infty$.

Mais alors $(k+1)^{2\phi(m)} \leqslant (k+1)^{m/5}$. Comme ce dernier terme est strictement inférieur à $k^{m/2}$ pour tout k suffisamment grand, cela conclut.

Solution de l'exercice 28 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 29 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 $a \geqslant 2$, 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 30 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 $3|a^2 + b^2 \Longrightarrow 3|a$ 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 $1 \leqslant x \leqslant 3^n - 1$ 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 $n \geqslant 1$, $1 \leqslant x \leqslant 3^n - 1$ et $3 \nmid x$.

Solution de l'exercice 31 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 $1 \leqslant i \leqslant k$. En particulier, cela implique que les nombres premiers $q_k; k \geqslant 1$ sont tous différents, et cela conclut.

Solution de l'exercice 32 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 $2^{2^n} \geqslant 4^n$ 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 $p_i \geqslant 5$), il existe un nombre premier q_A divisant N_A et ne divisant pas $2^j + 1$ pour $1 \leqslant j < \prod_{i \in A} p_i$ 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 33 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 $n \geqslant 2$ sont solution.

Solution de l'exercice 34 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 35 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 36 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 37 Comme $a = 1$ est solution, supposons maintenant $a \geqslant 2$. Il est clair qu'alors $n \geqslant p, q, r \geqslant 1$.

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 $(a, n, p, q, r) = (2, 6, 2, 2, 3), (2, 6, 2, 3, 2), (2, 6, 3, 2, 2)$.

Solution de l'exercice 38 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 $a \geqslant 3$, 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 39 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 40 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 $\dfrac{b^d - 1}{b - 1} \mid \dfrac{b^n - 1}{b - 1} = p^k$, ce qui est absurde.

Solution de l'exercice 41 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 42 Raisonnons par l'absurde en supposant que a_r, a_s, a_t appartiennent à une suite géométrique de raison $b \geqslant 2$, avec $r < s < t$. Alors

$$(3^r - 2^r)b^k = 3^s - 2^s, \qquad (3^s - 2^s)b^l = 3^t - 2^t \tag{12}$$

avec $k, l \geqslant 1$. 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 (12), p divise b. D'après la première égalité de (12), p divise alors $3^s - 2^s$, absurde.

Solution de l'exercice 43 Si $x = 0$, on vérifie que $y = 1, z = 2$ et que si $y = 0$, $x = 3$ et $z = 3$. On suppose donc $x, y \geqslant 1$. La suite est proche de l'exercice 38. 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 $y \geqslant 3$ 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 44 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 45 Comme dans la solution précédente de l'exercice 19, on commence par montrer que si $n > 2$ et $3^n - 2^n = p^k$ pour $k \geqslant 1$, 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 46 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 47 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 $q \geqslant 2$. 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 $(k+1)^q - 2 \geqslant kq$ diviseurs premiers différents de $a^{c^k} - b^{c^k}$.

Solution de l'exercice 48 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.

Solution de l'exercice 49 On prouve d'abord (i). La preuve qui suit est dûe à Roitman [8]. On commence par établir que pour tous entiers $a > 1, n > 2$, on a

$$\Phi_n(a) > a^{\frac{\sqrt{n}}{4}}. \tag{13}$$

Pour cela, montrons d'abord que $\Phi_n(a) > a^{\phi(n)/2}$. Déjà, si n est une puissance de 2, écrivons $n = 2^m$. Alors $\Phi_n(a) = a^{2^{m-1}} + 1 > a^{2^{m-1}} = a^{\phi(n)}$. Sinon, soit q un diviseur premier impair de n. On écrit n sous la forme $n = q^i N$ avec N premier avec q. Alors, en posant $b = a^{q^{i-1}}$ et en utilisant le Lemme 3,

$$\Phi_n(a) = \frac{\Phi_N\left(a^{q^i}\right)}{\Phi_N\left(a^{q^{i-1}}\right)} = \frac{\Phi_N(b^q)}{\Phi_N(b)} > \left(\frac{b^q - 1}{b+1}\right)^{\phi(N)} \geqslant \left(b^{q-2}(b-1)\right)^{\phi(N)} \geqslant (b^{q-2})^{\phi(N)} \geqslant \left(b^{\frac{q-1}{2}}\right)^{\phi(N)} = a^{\phi(n)/2}$$

où on a utilisé le fait que $b^q - 1 \geqslant b^{q-2}(b^2 - 1)$ pour la deuxième inégalité. Il suffit alors d'utiliser l'inégalité $\phi(n) \geqslant \sqrt{n}/2$. Celle-ci provient du fait que ϕ est multiplicative, combiné avec les inégalités $\phi(2^m) = 2^{m-1} \geqslant \sqrt{2^m}/2$ et $\phi(p^m) = (p-1)p^{m-1} \geqslant \sqrt{p^m}$ lorsque $p > 2$ est premier.

Revenons maintenant à l'exercice. Soient $a > 1$ et $n > 2$ tels qu'ils n'existe pas de diviseur premier primitif p de $a^n - 1$ tel que $|a^n - 1|_p > nN + 1$ (on va voir qu'il n'existe qu'un nombre fini de tels couples (a, n)). Soit p un diviseur premier primitif de $a^n - 1$ tel que $|a^n - 1|_p \leqslant nN + 1$. Ceci impose $p \leqslant nN + 1$. De plus, comme $\Phi_n(a)$ divise $a^n - 1$, on a

$$|\Phi_n(a)|_p \leqslant |a^n - 1|_p \leqslant nN + 1. \tag{14}$$

Ensuite, d'après le Lemme 7, $p \equiv 1 \pmod{n}$. Il existe donc au plus N diviseurs premiers primitifs p de $a^n - 1$ vérifiant $p \leqslant nN + 1$. Soit q le plus grand diviseur premier de n. En reprenant les notations de la preuve du théorème de Zsigmondy (comme $b = 1$, $\Psi_n = \Phi_n(a)$), on a

$$\Phi_n(a) \leqslant \lambda \cdot P_n \leqslant q \cdot P_n \leqslant n \cdot (nN + 1)^N,$$

où on a utilisé (14) pour la dernière inégalité. Mais alors, par (13), on obtient $a^{\frac{\sqrt{n}}{4}} \leqslant n(nN + 1)^N$. Comme il n'y a qu'un nombre fini de couples (a, n) avec $a > 1$ vérifiant cette inégalité, cela conclut.

Pour (ii), soit s un nombre premier divisant $a^n - 1$ et remarquons que $[a^n - 1]_p \geqslant |r^n - 1|_s$. Ainsi, si on fixe $N > 1$, d'après (i), pour tout entier $n \geqslant 1$ suffisamment grand, il existe un nombre premier s divisant $a^n - 1$ tel que $|a^n - 1|_s \geqslant nN + 1$, ce qui implique $\dfrac{[a^n - 1]_p}{n} > N$. Ceci conclut.

Références

[1] *http ://math.stackexchange.com/questions/660585/.*

[2] E. Artin, *The orders of the linear groups*, Comm. Pure Appl. Math., 8 (1955), pp. 355–365.

[3] A. Bang, *Taltheoretiske Undersøegelser*, Tidskrift for Math, 4(5) (1886), pp. 70–80,130–137.

[4] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of $a^n - b^n$*, Ann. of Math. (2), 5 (1904), pp. 173–180.

[5] L. E. Dickson, *On the Cyclotomic Function*, Amer. Math. Monthly, 12 (1905), pp. 86–89.

[6] E. Lucas, *Théorie des Fonctions Numériques Simplement Périodiques. [Continued]*, Amer. J. Math., 1 (1878), pp. 197–240.

[7] J. H. Maclagan-Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc., 6 (1905), pp. 349–352.

[8] M. Roitman, *On Zsigmondy primes*, Proc. Amer. Math. Soc., 125 (1997), pp. 1913–1919.

[9] M. Teleuca, *Zsigmondy's theorem and its applications in contest problems*, Internat. J. Math. Ed. Sci. Tech., 44 (2013), pp. 443–451.

[10] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys., 3 (1892), pp. 265–284.