DOMAINE : Arithmétique
NIVEAU : Avancé
CONTENU : Cours et exercices

AUTEUR : Igor KORTCHEMSKI
STAGE : Montpellier 2014

Autour de $a^n \pm b^n$

Ce cours présente des résultats concernant l'étude des facteurs premiers de $a^n \pm b^n$ autour de trois thèmes :

(i) le théorème LTE ("Lifting The Exponent"), qui permet (sous certaines hypothèses) de trouver la plus grande puissance d'un nombre premier divisant $a^n \pm b^n$,

(ii) les polynômes cyclotomiques, qui interviennent en arithmétique en lien avec la notion d'ordre d'un élément modulo un nombre premier,

(iii) et enfin le théorème de Zsigmondy, qui s'intéresse aux facteurs premiers de $a^n - b^n$ qui ne divisent aucun des entiers $a^j - b^j$ pour $1 \leqslant i \leqslant j$. Ce théorème s'énonce simplement, mais sa démonstration est délicate. Comme celle-ci n'utilise que des notions élémentaires combinées avec (i) et (ii) et qu'elle est instructive, nous avons jugé intéressant de la présenter dans sa totalité.

Nous supposons ici acquis :

(i) la notion d'ordre d'un entier modulo un nombre premier (on rappelle que si a et n sont des entiers premiers entre eux, l'ordre de a modulo n est le plus petit entier $\omega \geqslant 1$ tel que $a^\omega \equiv 1 \pmod{n}$. Cela entraîne que si $a^k \equiv 1 \pmod{n}$, alors ω divise k).

(ii) la notion de nombre complexe, en particulier l'écriture sous la forme $re^{i\theta}$ et la notion de module, et renvoyons à un cours sur les nombres complexes pour ces prérequis.

1 Théorème LTE

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

On commence par le lemme suivant.

Lemme 1. Soient x, y des entiers relatifs 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 $nx^{n-1} \not\equiv 0 \pmod{p}$. Donc p ne divise pas $x^{n-1} + yx^{n-2} + \cdots + y^{n-1}$ et le résultat en découle. □

Théorème 2 (Théorème LTE)**.** Soit p un nombre premier **impair**. Soient a, b des nombres entiers relatifs et un entier $n \geqslant 1$. On suppose que p divise $a - b$ mais que $p \nmid x, p \nmid y$. Alors :

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

Démonstration. **Étape 1.** On montre d'abord que

$$v_p(x^p - y^p) = v_p(x - y) + 1. \tag{1}$$

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

$$\begin{aligned} y^i x^{p-1-i} &= (x + kp)^i x^{p-1-i} \\ &= \left(x^i + ikpx^{i-1} + \sum_{j=2}^{i} \binom{j}{i} (kp)^j x^{i-j} \right) x^{p-1-i} \\ &\equiv x^{p-1} + ikpx^{p-2} \pmod{p^2}. \end{aligned}$$

Il en découle que

$$\begin{aligned}
\sum_{i=0}^{p-1} y^i x^{p-1-i} &\equiv \sum_{i=0}^{p-1} \left(x^{p-1} + ikpx^{p-2}\right) \pmod{p^2} \\
&\equiv px^{p-1} + \frac{p-1}{2} \cdot kp^2 x^{p-2} \pmod{p^2} \quad \left(\frac{p-1}{2} \text{ est entier car } p \text{ est imp}\right. \\
&\equiv px^{p-1} \pmod{p^2} \\
&\not\equiv 0 \pmod{p^2} \qquad (\text{car } p \nmid x).
\end{aligned}$$

Ceci établit (1) .

Étape 2. Par une récurrence immédiate, on obtient que

$$v_p(x^{p^i} - y^{p^j}) = v_p(x-y) + i. \tag{2}$$

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

$$\begin{aligned}
v_p(x^n - y^n) &= v_p\left(\left(x^{p^\alpha}\right)^N - \left(y^{p^\alpha}\right)^N\right) \\
&= v_p(x^{p^\alpha} - x^{p^\alpha}) \qquad \text{(d'après le Lemme 1)} \\
&= v_p(x-y) + \alpha \qquad \text{(d'après (2)).}
\end{aligned}$$

Ceci conclut la preuve. □

Lorsque n est impair, en changeant y en $-y$ 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 :

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

Ce théorème et son corollaire doivent être connus. Insistons sur le fait que p doit être impair pour appliquer le théorème LTE. On renvoie à
http ://www.artofproblemsolving.com/Resources/Papers/LTE.pdf
pour des extensions au cas $p = 2$ et de nombreux autres exemples d'application. Nous ne pouvons qu'encourager fortement le lecteur à lire attentivement ce dernier texte.

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 $p \geqslant 3$. On vérifie réciproquement que $p = 3$ convient aussi.

- Exercices -

Exercice 1 Soient a, n deux entiers strictement positifs et p un nombre premier impair tel que $a^p \equiv 1 \bmod p^n$. Montrer que $a \equiv 1 \bmod p^{n-1}$.

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 Soit p un premier impair et m un entier tel qu'il existe des entiers $x, y > 1$ vérifiant

$$\frac{x^p + y^p}{2} = \left(\frac{x+y}{2}\right)^m.$$

Montrer que $m = p$.

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

Exercice 5 (IMO 1990/3) Trouver tous les entiers $n \geqslant 1$ tels que n^2 divise $2^n + 1$.

Exercice 6 (Bulgarie 1997) Pour un entier $n > 0$, $3^n - 2^n$ est la puissance d'un nombre premier. Montrer que n est premier.

Exercice 7 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.

2 Un lemme utile

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

Lemme 4. Soient $a \neq b$ des entiers relatifs premiers entre eux. Soient $m, n \geqslant 1$ des entiers. Alors

$$a^n - b^n \wedge a^m - b^m = \left|a^{m\wedge n} - b^{m\wedge n}\right|.$$

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 $m \wedge n$ divise m, $V_{m\wedge n}$ divise V_m. De même, $V_{m\wedge n}$ divise V_n. On en déduit que $V_{m\wedge n}$ divise $V_m \wedge V_n$.

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 $V_m \wedge V_n$ divise $a^n V_{m-n}$. Comme a et b sont premiers entre eux, $V_m \wedge V_n$ divise V_{m-n}. Ainsi, $V_m \wedge V_n$ divise $V_{m-n} \wedge V_n$.

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

3 Polynômes cyclotomiques

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

3.1 Racines primitives de l'unité

Définition 5. 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 $0 \leqslant k \leqslant n-1$. On notera Ω_n l'ensemble des racines n-ièmes de l'unité. Si $z \in \cup_{n\geqslant 1}\Omega_n$, 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 $\omega(z)$. 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).

On laisse la preuve de la proposition suivante en exercice, qui se démontre comme la proposition similaire concernant l'ordre modulo un entier (ou, si on préfère, découle du fait que les groupes $(\Omega_n, \times)$ et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont isomorphes).

Proposition 6. Soit $z \in \Omega_n$. Alors :

(i) $\omega(z)$ divise n.

(ii) Si $z^k = 1$, alors $\omega(z)$ divise k.

Lemme 7. Soit z une racine primitive n-ième. Alors $\Omega_n = \{z, z^2, \dots, z^{n-1}\}$.

Démonstration. L'ordre de z étant égal à n, l'ensemble $\{z, z^2, \dots, z^{n-1}\}$ est constitué de n éléments distincts, et a donc le même cardinal que Ω_n. Il suffit donc de montrer que $\{z, z^2, \dots, z^{n-1}\} \subset \Omega_n$. Soit donc $1 \leqslant i \leqslant n$. Comme $(z^i)^n = (z^n)^i = 1$, on bien $z^i \in \Omega_n$. Ceci conclut. □

Proposition 8. Soit z une racine de l'unité. Alors $\omega(z^k) = \frac{\omega(z)}{k \wedge \omega(z)}$. En particulier, si z est une racine primitive n-ième, alors z^k est une racine primitive $n/k \wedge n$-ième.

Démonstration. Tout d'abord, on a bien $(z^k)^{n/k \wedge n} = (z^n)^{k/k \wedge n} = 1$. Ensuite, si $(z^k)^m = 1$ pour un entier $m \geqslant 1$, on a $z^{km} = 1$ et donc n divise km d'après la Proposition 8. On écrit ensuite $k = k \wedge n \cdot K$ et $n = k \wedge n \cdot N$, avec K et N premiers entre eux. Comme n divise km, on en déduit que N divise Km et donc N, premier avec K, divise m. Donc $n/k \wedge n$ divise m, ce qui montre que $n/k \wedge n$ divise $\omega(z^k)$ et conclut. □

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 $n-1$ premiers avec n, et que $\phi(ab) = \phi(a)\phi(b)$ lorsque a et b sont des entiers premiers entre eux. Du Lemme 7 et de la Proposition 8, il vient immédiatement le corollaire suivant.

Corollaire 9. Il existe $\phi(n)$ racines n-ièmes de l'unité.

3.2 Fonction de Möbius

Définition 10. Soit $\mu : \mathbb{N} \to \{-1, 0, 1\}$ la fonction définie comme suit :

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n \text{ n'est pas divisible par un carré et } k \text{ est le nombre de facteurs p} \\ 1 & \text{sinon.} \end{cases}$$

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.

Lemme 11. Soit $n \geqslant 1$. Alors

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geqslant 2. \end{cases}$$

Démonstration. Pour $n = 1$, c'est vrai. On suppose donc $n \geqslant 2$ et on note T le produit des nombres premiers divisant n. Si d divise n, il est clair que $\mu(d) = 0$ si d ne divise pas T. Soit ensuite p un nombre premier quelconque divisant T et posons $T = pT'$. Alors

$$\sum_{d \mid n} \mu(d) = \sum_{d \mid T} \mu(d) = \sum_{d \mid pT'} \mu(d) = \sum_{d \mid T'} (\mu(d) + \mu(pd)) = \sum_{d \mid T'} (\mu(d) - \mu(d)) = 0.$$

□

L'utilité de la fonction de Möbius provient, entre autres, grâce au théorème d'inversion suivant.

Théorème 12 (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 $n \geqslant 1$.

Démonstration. Posons

$$A = \prod_{d \mid n} F\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d \mid n} \prod_{t \mid \frac{n}{d}} f(t)^{\mu(d)}.$$

Or ($d \mid n$ et $t \mid \frac{n}{d}$) est équivalent à ($t \mid n, d \mid n, t \mid \frac{n}{d}$). Donc

$$A = \prod_{t \mid n} \prod_{d \mid n, t \mid \frac{n}{d}} f(t)^{\mu(d)} = \prod_{t \mid n} f(t)^{\sum_{d \mid n, t \mid \frac{n}{d}} \mu(d)}.$$

Or, pour un diviseur t de n, ($d \mid n$ et $t \mid \frac{n}{d}$) est équivalent à $d \mid \frac{n}{t}$. Donc

$$\sum_{d \mid n, t \mid \frac{n}{d}} \mu(d) = \sum_{d \mid \frac{n}{t}} \mu(d).$$

D'après le Lemme 11, cette somme est nulle sauf si $t = n$. En déduit que $A = f(n)$. □

3.3 Définition et premières propriétés

Définition 13. 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. Nous verrons plus loin que Φ est en fait à coefficients entiers.

Théorème 14. Pour tout entier $n \geqslant 1$, on a $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Démonstration. Pour simplifier les notations, posons $P(X) = X^n - 1$ et $Q(X) = \prod_{d|n} \Phi_d(X)$. Comme P et Q sont unitaires, que les racines de P sont toutes différentes et que les racines de Q sont aussi toutes différentes, il suffit de montrer que les racines de P et Q sont les mêmes. D'abord, si $z^n = 1$, soit $d = \omega(z)$. Alors $d \mid n$ et z est racine primitive d-ièm et donc $\Phi_d(z) = 0$, de sorte que $Q(z) = 0$. Réciproquement, si $Q(z) = 0$, on a bien $z^n = 1$ et donc $P(z) = 0$. Ceci conclut. □

En prenant les degrés dans l'égalité du théorème précédent, on obtient le résultat suivant.

Corollaire 15. Pour tout entier $n \geqslant 1$, on a $n = \sum_{d|n} \phi(d)$.

Un autre corollaire utile, qui est une conséquence immédiate, est le suivant.

Corollaire 16. Soient $n \geqslant 1$ un entier, $a \in \mathbb{Z}$ et p un nombre premier. Si p divise $X^n - 1$, alors il existe un diviseur d de n tel que p divise $\Phi_d(a)$.

On déduit aussi du théorème 14 le résultat important qui suit.

Corollaire 17. Pour tout entier $n \geqslant 1$, le polynôme Φ_n est à coefficients entiers.

Démonstration. On raisonne par récurrence forte sur n. Pour $n = 1$, on a bien $\Phi_1(X) = X - 1$. Supposons que $\Phi_k \in \mathbb{Z}[X]$ pour tout $1 \leqslant k \leqslant n - 1$. Posons alors

$$Q(X) = \prod_{d|n, d \neq n} \Phi_d(X),$$

qui est à coefficients entiers, unitaire. Par division euclidienne de X^n-1 par Q, on en déduit l'existence de polynômes $P, R \in \mathbb{Z}[X]$ tels que $X^n-1 = P(X)Q(X)+R(X)$ avec $\deg R < \deg Q$. En utilisant le théorème 14, on en déduit que

$$R(X) = Q(X)\left(P(X) - \Phi_n(X)\right).$$

Comme $\deg R < \deg Q$, on a forcément $R = 0$ et $\phi_n(X) = P(X) \in \mathbb{Z}[X]$. □

Corollaire 18. Si $n \geqslant 1$ est impair, on a $X^n + 1 = \prod_{d|n} \Phi_{2d}(X)$.

Démonstration. D'après le Théorème 14, on a

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

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

Lemme 19 (Encadrement des polynômes cyclotomiques)**.** Soit $a \in \mathbb{C}$ et $n \geqslant 1$. On a

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

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-ième ne sont pas alignées, ce qui implique l'existence d'une racine primitive n-ième z telle que $|a| - 1 < |z - a| < |a| + 1$. □

On va maintenant présenter quelques résultats permettant de calculer en pratique les polynômes cyclotomiques.

Théorème 20 (Factorisation des polynômes cyclotomiques)**.** Pour tout entier $n \geqslant 1$, on a

$$\Phi_n(X) = \prod_{d|n} \left(X^{\frac{n}{d}} - 1\right)^{\mu(d)}.$$

Compte tenu du Théorème 14, ce théorème est une conséquence immédiate du théorème 12. En prenant les degrés dans l'égalité du théorème précédent, on en déduit la formule suivante.

Corollaire 21. Pour tout entier $n \geqslant 1$, on a $\phi(n) = \sum_{d|n} \frac{n}{d}\mu(d)$.

Dans le cas où n est un nombre premier, le théorème 20 fournit

Corollaire 22. Soit p un nombre premier. Alors

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Théorème 23. Si p est un nombre premier et $n \geqslant 1$ un entiers, on a

$$\Phi_{pn}(X) = \begin{cases} \Phi_n(X^p) & \text{si } p \mid n \\ \dfrac{\Phi_n(X^p)}{\Phi_n(X)} & \text{si } p \nmid n. \end{cases}$$

Démonstration. On pourrait prouver ce résultat en utilisant le Théorème 20, mais nous poursuivons ici une autre approche. Supposons d'abord que p divise n et écrivons $n = p^k N$ avec p ne divisant pas N. On remarque que les racines du polynôme de gauche de l'égalité du Théorème sont toutes différentes, et que c'est également le cas pour celui de droite. Montrons que les deux polynômes ont même degré. On a $\deg \Phi_{pn} = \phi(p^{k+1}N) = p^k(p-1)\phi(N)$. De plus, $\deg \Phi_n(X^p) = p\phi(n) = p\phi(p^k N) = p^k(p-1)\phi(N)$. Pour montrer que $\Phi_{pn}(X) = \Phi_n(X^o)$, il suffit donc de montrer que si $\Phi_{pn}(z) = 0$ alors $\Phi_n(z^p) = 0$. Pour cela, soit z une racine pn-ième. D'après la Proposition 8, z^p est racine $pn/p \wedge pn = n$-ième de l'unité, donc est racine de Φ_n.

Si p ne divise pas n, on vérifie de même que les degrés coincident. De plus, si $\Phi_{pn}(z) = 0$, alors z^p est racine n-ième de l'unité et $z^n \neq 1$, de sorte que z est bien racine de $\Phi_n(X^p)/\Phi_n(X)$. □

Par récurrence immédiate, on obtient alors le résultat suivant.

Corollaire 24. Si p est un nombre premier et $k, n \geqslant 1$ sont des entiers, on a

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

Corollaire 25. Si $n \geqslant 1$ est un entier impair, alors $\Phi_{2n}(X) = \Phi_n(-X)$.

Démonstration. D'après le théorème 23, on a $\Phi_{2n}(X) = \Phi_n(X^2)/\Phi_n(X)$. Or $\Phi_n(X^2) = \Phi_n(X) \cdot \Phi_n(-X)$. 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. □

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

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

Théorème 26. Si $a, n \geqslant 1$ sont des entiers premiers entre eux, alors $\Phi_n(X^a) = \prod_{d|a} \Phi_{nd}(X)$.

Démonstration. En utilisant le corollaire 15, on vérifie que les degrés des deux polynômes unitaires de part et d'autre de l'égalité 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 8 :

$$n \cdot a \wedge \omega(z) = \omega(z). \tag{3}$$

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

Remarque 27. Il est possible de montrer que $\Phi_n(X)$ est irréductible sur $\mathbb{Q}[X]$ pour tout entier $n \geqslant 1$, de sorte que le Théorème 14 fournit la décomposition en polynômes irréductibles de $X^n - 1$ sur $\mathbb{Q}[X]$.

3.4 Propriétés d'ordre

Lemme 28. Soient $a, n \geqslant 1$ des entiers et p un nombre premier. Supposons qu'il existe un polynôme $P \in \mathbb{Z}_p[X]$ tel que l'égalité

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

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

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

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

On évalue en $X = a$ pour obtenir que $na^{n-1} = 0$ dans $\mathbb{Z}_p[X]$. Donc p divise na^{n-1} Or 0 n'est pas racine de $X^n - 1$ dans $\mathbb{Z}_p[X]$, 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 29. 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 $\Phi_d(a)$, cela signifie que a est racine de Φ_d dans $\mathbb{Z}_p[X]$. Donc il existe un polynôme $P_1 \in \mathbb{Z}_p[X]$ tel que $\Phi_d(X) = (X - a)P_1(X)$ dans $\mathbb{Z}_p[X]$. De même, il existe un polynôme $P_2 \in \mathbb{Z}_p[X]$ tel que $\Phi_n(X) = (X - a)P_2(X)$ dans $\mathbb{Z}_p[X]$. D'après le Théorème 14, on a $X^n - 1 = (X - a)^2 R(X)$ dans $\mathbb{Z}_p[X]$ pour un certain polynôme $R \in \mathbb{Z}_p[X]$. Le Lemme 29 implique alors que p divise n. □

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

Théorème 30. 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, $\Phi_m(a) \wedge \Phi_n(a)$ 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 le Théorème 23,

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

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 $g = M \wedge N$. On a

$$p \mid \Phi_M(a) - 1 \mid a^M - 1, \qquad p \mid \Phi_N(a) - 1 \mid a^N - 1.$$

Donc

$$p \mid a^M - 1 \wedge a^N - 1 | a^g - 1$$

d'après le Lemme 4. Le Corollaire 16 forunit 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 29, ceci implique que p divise M, ce qui est absurde. Le fait que $\Phi_m(a) \wedge \Phi_n(a)$ soit une puissance de p est une conséquence immédiate de la première assertion. □

On peut remarquer que le Lemme 29 est un cas particulier du théorème 30.

Théorème 31. 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, $\omega_p(a) = n$.

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 16 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 29, 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 16 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 30, 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 16, 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 32. Si p, q sont deux nombres premiers tels que q divise $1 + x + \cdots + x^{p-1}$, alors $q \equiv 1 \pmod{p}$ ou $q = p$.

3.5 Applications

Théorème 33 (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 31 (i), ou bien $p \equiv 1 \pmod{T}$, ou bien p divise n. Or $p \mid \Phi_n(T^k) \mid T^{nk} - 1$, donc p est premier T. Donc p est premier avec n, ce qui implique $p \equiv 1 \pmod{T}$ et ce qui est absurde. □

Voici maintenant quelques exercices d'application.

Exercice 1 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.

Exercice 2 (D'après Shortlist IMO 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 3 (Iran 2013) Soit p un nombre premier et d un diviseur de $p - 1$. Trouver tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ dont l'ordre vaut d.

Exercice 4 (Shortlist IMO 2006) Trouver tous les entiers relatifs x, y tels que

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

Exercice 5 Prouver qu'il existe une infinité d'entiers positifs n tels que tous les diviseurs premiers de $n^2 + n + 1$ sont tous inférieurs ou égaux à $\sqrt{n}$.

4 Théorème de Zsigmondy

Soient $a, b \in \mathbb{Z}$ et $n \geqslant 2$ un entier. Un diviseur premier p de $a^n - b^n$ est dit *primitif* si, pour tout entier $1 \leqslant j \leqslant n$, p ne divise pas $a^j - b^j$, et *non primitif* sinon.

Par exemple, 5 est un diviseur primitif de $2^4 - 1$, 3 n'est pas diviseur primitif de $2^3 - 1$, et $2^6 - 1^6$ n'admet pas de diviseur premier primitif.

Le Théorème de Zsigmondy établit l'existence de diviseurs premiers primitifs, sauf exceptions.

Théorème 34 (Théorème de Zsigmondy)**.** 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 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.

En prenant $b = 1$, ceci implique en particulier l'existence d'un nombre premier p tel que l'ordre de a modulo p soit égal à n.

On peut aussi aisément en déduire la version suivante :

Théorème 35 (Théorème de Zsigmondy bis)**.** Soient $a > b$ 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 $1 \leqslant k \leqslant n$, 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 34. 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 34 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 supposera $n > 2$.

- Quelques propriétés des diviseurs premiers primitifs -

Lemme 36. Soit p un nombre premier divisant $a^n - b^n$. Alors p est non primitif si, et seulement si, il existe un diviseur $d \mid n$ 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 $d = k \wedge n$. En particulier, $d \mid n$ et $d < n$. En utilisant le Lemme 4, on obtient

$$p \mid a^n - b^n \wedge a^k - b^k = a^d - b^d.$$

□

Lemme 37. 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 théorème de Fermat, $c^{p-1} \equiv 1 \pmod{p}$, et donc n divise $p - 1$. □

- 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 31 (iii), il est naturel de considérer $\Phi_n(a)$.

L'identité clé est la suivante :

$$a^n - b^n = \prod_{d \mid n} \Psi_n. \tag{4}$$

Pour la prouver, on écrit, en utilisant le Théorème 14 et le corollaire qui le suit,

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

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

$$\Psi_n = \prod_{d \mid n} \left(a^{\frac{n}{d}} - b^{\frac{n}{d}} \right)^{\mu(d)}. \tag{5}$$

en vertu du Théorème 12.

On utilisera aussi l'inégalité suivante :

$$(a - b)^{\phi(n)} < \Psi_n < (a + b)^{\phi(n)}, \tag{6}$$

avec inégalités strictes car $n > 2$. Cela se démontre exactement comme le Lemme 19 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

$$\Psi_n(a, b) = \frac{\Psi_N\left(a^{p^\alpha}, b^{p^\alpha}\right)}{\Psi_N\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right)}, \qquad \Psi_n(a, b) = \Psi_{pN}\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right). \tag{7}$$

Cela se démontre aisément en utilisant le Corollaire 24 ; montrons par exemple la première égalité en utilisant le fait que $\phi(p^\alpha N) = \phi(p^\alpha)\phi(N) = p^{\alpha-1}(p - A)\phi(N)$:

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

La deuxième égalité apparaissant dans (7) se démontre de la même manière. Pour simplifier, on écrira Ψ_n à la place de $\Psi_n(a, b)$.

- Preuve du Théorème 34 -

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

$$P_n = p_{i_1}^{\alpha_1} \cdots p_{i_j}^{\alpha_j},$$

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 est un diviseur premier primitif de $a^n - b^n$. D'après le Lemme 36, 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 (4). On en déduit que p est premier avec $\prod_{d|n,d\neq n} \Psi_d$. Par (4), 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

$$\Psi_n = \lambda \cdot P_n. \tag{8}$$

Tout d'abord, on remarque qu'on a bien $P_n > 1$ dans le cas $\lambda = 1$. En effet, d'après (6), 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. On montre que :

(i) Si $p \mid \lambda$, alors p n'est pas primitif. En particulier, $\lambda \wedge P_n = 1$.

(ii) Si $p \mid \lambda$, alors $p \mid n$.

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

Pour (ii), supposons que $p \mid \lambda$. Par (i), p n'est pas primitif, et d'après le Lemme 36, il existe $d_0 \neq n$ tel que $d_0 \mid n$ et $p \mid a^{d_0} - b^{d_0}$. Compte tenu de (4), on a

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

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 (7),

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

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

$$p \equiv 1 \pmod{N} \tag{9}$$

par le Lemme 37. 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 $\lambda \wedge P_n = 1$ (d'après l'étape 2), il suffit de montrer que $\nu_p(\Psi_n) = 1$.

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 31 (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 (5). 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 (5) entraîne que

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

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

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 $\nu_2(\Psi_n) = 1$. □

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 (8) et (6), 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 (7) et (6), on a

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

ce qui est absurde.

Deuxième cas : $\alpha = 1$. On remarque d'abord que $a^p - b^p \geqslant a + b$ car

$$a^p - b^p = \sum_{i=1}^{p} \binom{p}{i} b^i \geqslant pb + b^p \geqslant 2b + 1.$$

Alors, en vertu de successivement (7) et (6), on a

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

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

La congruence (9) 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.

- Exercices -

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

Exercice 7 Trouver tous les entiers positifs (x, y, n, k) tels que x et y soient premiers entre eux et tels que

$$3^n = x^k + y^k.$$

Exercice 8 (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 9 (D'après IMO Shortlist 2002) Soit $n \geqslant 1$ un entier et soient $p_1, p_2, \ldots, p_n$ des nombres premiers 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 (IMO shortlist 2004 N4) Trouver tous les entiers strictement positifs a, m, n tels que $a^m + 1$ divise $(a+1)^n$.

Exercice 11 (Etats-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 Tchèquo-Slovaque 1996) Trouver tous les entiers strictement positifs x, y, p tels que $p^x - y^p = 1$ avec p premier.

Exercice 13 (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 (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 (BMO 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 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 18 (Roumanie TST 1994) Montrer que la suite $a_n = 3^n - 2^n$ ne contient pas trois termes d'une même suite géométrique.

Exercice 19 (Angleterre 1996) Trouver les entiers positifs x, y, z tels que $2^x + 3^y = z^2$.

Exercice 20 Résoudre l'exercice 4 en vous aidant du théorème de Zsigmondy, qui, pour rappel, demandait de trouver toutes les solutions entières de

$$x^{2009} + y^{2009} = 7^k$$

Exercice 21 Résoudre l'exercice 6 en vous aidant du théorème de Zsigmondy, dont l'énoncé est le suivant pour rappel. Pour un entier $n > 0$, $3^n - 2^n$ est la puissance d'un nombre premier. Montrer que n est premier.

Exercice 22 (Shortlist 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 23 (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.

5 Solution 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, $a^{p-1} \equiv 1 \bmod p$. Comme $a^p \equiv 1 \bmod p$, on en déduit que $a \equiv 1 \bmod p$. 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 $4^n - 1$. Comme 3 divise $4 - 1$, on peut appliquer le théorème LTE :

$$v_3(4-1) + v_3(n) = v_3(4^n - 1) \geqslant k.$$

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

$$\frac{x^p + y^p}{2} \geqslant \left(\frac{x+y}{2}\right)^p.$$

Comme $\frac{x^p+y^p}{2} = \left(\frac{x+y}{2}\right)^m$, il s'ensuit que $m \geqslant p$. Soit $d = pgcd(x, y)$, $x = dX$, $y = dY$. L'équation se réécrit

$$2^{m-1}(X^p + Y^p) = d^{m-p}(X+Y)^m. \tag{10}$$

Soit q un diviseur premier impair de $X+Y$. Par le théorème LTE, $v_q(X^p+Y^p) = v_q(X+Y) + v_q(p)$ et d'autre part $v_q(d^{m-p}(X+Y)^m) \geqslant m v_q(x+y)$. Donc $m \geqslant 2$ et $p \geqslant 2$, ce qui aboutit à une contradiction.

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 (10), on obtient

$$m - 1 + v_2(X+Y) \geqslant m v_2(X+Y),$$

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 possibles.

<u>*Solution de l'exercice 5*</u> Montrons que si n divise $2^n + 1$, alors n est une puissance de 3. Il est clair que n est impair. Ensuite, en considérant p le plus petit facteur premier de n, des considérations sur l'ordre de 2 modulo p donnent $p = 3$. En effet, si r est l'ordre de 2 modulo p, alors $2^{2n} \equiv 1 \pmod{p}$, et donc r divise $2n$. D'après le petit théorème de Fermat, $2^{p-1} \equiv 1 \pmod{p}$, et donc r divise $p - 1$. Par définition de p, on en déduit que $r = 2$. Ainsi, $4 \equiv 1 \pmod{p}$ ce qui force $p = 3$.

Écrivons alors $n = 3^k u$ avec u non divisible par 3. Le même raisonnement montre que si $u > 1$ alors le plus petit facteur premier de u est 3. On en déduit que n est une puissance de 3.

On applique le théorème LTE (n est impair) :

$$v_3(2^n + 1) = v_3(2 + 1) + v_3(n) = k + 1.$$

Or $v_3(n^2) = 2k$ et n^2 divise 2^n+1. On en déduit que $2k \leqslant k+1$, ce qui donne $k = 0$ ou $k = 1$. Notons que ce dernier résultat peut aussi se démontrer de manière immédiate en regardant les puissances de 2 modulo 9. Réciproquement, $n = 1$ et $n = 3$ sont bien solution.

<u>*Solution de l'exercice 6*</u> 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 :

$$3^{n'} + 2^{n'} = p^\alpha, \qquad 3^{n'} - 2^{n'} = p^\beta.$$

Alors $2^{n'+1} = p^\beta(p^{\alpha-\beta} - 1)$. Donc $p = 2$, ce qui est absurde. 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 le théorème 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 forcément premier.

<u>*Solution de l'exercice 7*</u> Il est clair que $a = 1$ convient. Montrons que c'est le seul. Supposons donc $a > 1$. Choisissons $n = 2m$ et remarquons que $a^2 + 1$ n'est pas une puissance de 2 car congru à 1 ou 2 modulo 4. Soit donc p un nombre premier impair tel que p divise a^2+1. Alors d'après le théorème LTE :

$$v_p(4(a^n + 1)) = v_p(a^2 + 1) + v_p(m).$$

On choisit m de sorte que ce dernier terme soit congru à 1 modulo 3. Alors $4(a^n + 1)$ ne peut pas être un cube, contradiction.

<u>*Solution de l'exercice 8*</u> On commence par remarquer que

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

D'après le lemme 19, 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 30, d/d' est une puissance de p, donc $p = 2$. Or d'après le Théorème 14 le coefficient constant d'un polynôme cyclotomique vaut ± 1 (on peut en fait montrer qu'il vaut 1, voir la solution de l'exercice 3), donc 2 ne peut pas diviser $\Phi_{3d}(2)$. Ceci conclut

<u>*Solution de l'exercice 9*</u> On va montrer que $2^{p_1 p_2 \cdots p_n}+1$ a au moins 2^{n-1} diviseurs premiers distincts, ce qui concluera. D'après le Corollaire 18, on a

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

D'après le Théorème 30, 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 19 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 10 Le problème revient à calculer $\Phi_d(0)$, qui vaut 1 car les racines de Φ_d, de module 1, peuvent être réparties en couples de racines conjugées.

Solution de l'exercice 11 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 32, n'importe quel diviseur premier de $1 + x + \cdots + x^6$ est soit égal à 7, soit est congru à 1 modulo 7. Ainsi, n'importe quel 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 12 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 le Théorème 26,

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

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 19, 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 $\sum_{n \geqslant 1} \frac{1}{p_i}$ 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 13 On réécrit l'équation sous la forme $19^a - 2^a = p^b$. Comme 17 divise le terme de gauche, on a forcément $p = 17$. 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 14 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 $(x, y, k) \neq (2, 1, 3)$, 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. La seule solution est donc $(x, y, k) = (2, 1, 3)$.

Solution de l'exercice 15 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 nombre premiers $q_k; k \geqslant 1$ sont tous différents, et cela conclut.

Solution de l'exercice 16 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 17 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 18 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 19 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 est 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 20 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 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 21 Tout d'abord, il est clair que $n \geqslant p, q, r \geqslant 1$. Comme $a = 1$ est solution, supposons maintenant $a \geqslant 2$.

Si l'un des entiers p, q, r sont égaux à n, on a forcément $a = 2$ et les deux autres sont égaux à 1. On trouve donc les solutions $(a, n, p, q, r) = (2, n, 1, 1, n), (2, n, 1$ 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 22 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 23 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 24 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 :

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

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,

$$3 \cdot 7 \cdot 15 \cdots (a^{n+1} - 1) = 63,$$

qui ne fournit pas d'autre solution.

Solution de l'exercice 25 Raisonnons par l'absurde en supposant que a_r, a_s, a_t appartiennent à une suite géométrique de raison b, avec $r < s < t$. Alors

$$(3^r - 2^r)b^{s-r} = 3^s - 2^s, \qquad (3^s - 2^s)b^{t-s} = 3^t - 2^t. \tag{11}$$

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 (11), p divise b. D'après la première égalité de (11), p divise alors $3^s - 2^s$, absurde.

Solution de l'exercice 26 Si $x = 0$, on vérifie que forcément $y = 1, z = 2$ et que si $y = 0$, forcément $x = 3$ et $z = 3$. On suppose donc $x, y \geqslant 1$. 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 $y \geqslant 3$ 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 27 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 28 Comme dans la solution précédente de l'exercice 6, 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 29 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 deux, ce qui était demandé.

Solution de l'exercice 30 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 $a^i - b^i$.