EXERCICES SUR LES POLYNÔMES CYCLOTOMIQUES

Igor Kortchemski

- Rappels de cours -

Le n-ième polynôme cyclotomique Φ_n est défini par

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

Il est de degré $\phi(n)$ (avec ϕ la fonction d'Euler), à coefficients entiers, et vérifie $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Rappelons quelques propriétés utiles des polynômes cyclotomiques :

(1) [Factorisations] Pour tout entier $n \geq 1$, on a

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

où $\mu : \mathbb{N} \to \{-1, 0, 1\}$ est la fonction de Möbius définie comme suit :

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

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

Si p est un nombre premier et $n \geq 1$ un entier, on a

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1 \qquad \text{et} \qquad \Phi_{pn}(X) = \begin{cases} \Phi_n(X^p) & \text{si } p \mid n \\ \dfrac{\Phi_n(X^p)}{\Phi_n(X)} & \text{si } p \nmid n. \end{cases}$$

Si p est un nombre premier et $k, n \geq 1$ sont des entiers, on a

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

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

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

(2) [Encadrements] Soient $a \in \mathbb{C}$ et $n \geq 1$. On a

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

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

En lien avec l'arithmétique, les résultats suivants sont les plus souvent utilisés :

(3) Soient $m, n \geq 1$ 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, $PGCD(\Phi_m(a), \Phi_n(a))$ est une puissance de p.

(4) Soit p un nombre premier, $n \geq 1$ 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.

- Exercices -

Exercice 1 Soit $n \geq 2$. Il existe une infinité de nombres premiers p tels que $p \equiv 1 \pmod{n}$.

Exercice 2 Soit p un nombre premier. Montrer que $p^p - 1$ admet un diviseur premier congru à 1 modulo p.

Exercice 3 Soient $n, b \geq 2$ des entiers. Montrer que si $(b^n - 1)/(b - 1)$ est une puissance d'un nombre premier, alors n est une puissance d'un nombre premier.

Exercice 4 Soit $n \geq 1$ 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 $n \geq 1$ tel que $2^{2^n} + 2^{2^{n-1}} + 1$ est divisible par au moins $n + 1$ nombres premiers différents ?

Exercice 5 (Liste courte Olympiades Internationales de Mathématiques 2002) Soit $n \geq 1$ 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 6 (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 7 (Liste courte Olympiades Internationales de Mathématiques 2006) Trouver tous les entiers relatifs x, y tels que $\frac{x^7-1}{x-1} = y^5 - 1$.

Exercice 8 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 $\sqrt{n}$.

Solution de l'exercice 1 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 $k \geq 1$ tel que $\Phi_n(T^k) > 1$. Soit alors p un diviseur premier de $\Phi_n(T^k)$. D'après le point (4) (i) des rappels, 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.

Solution de l'exercice 2 Soit q un diviseur premier de $(p^p - 1)/(p - 1) = \Phi_p(p)$. D'après le point (4) des rappels, 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 3 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 point (3) des rappels, 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 4 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 point (2) des rappels, 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 point (3) des rappels, 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 $n_0 \geq 1$ 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 $n_0 \geq 1$ 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 $n_0 \geq 2$, 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 5 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. Comme $X^n + 1 = \prod_{d \mid n} \Phi_{2d}(X)$ lorsque n est impair, 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 point (3) des rappels, 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 point (2) des rappels 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 6 D'après le point (3) (iii) des rappels, 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 7 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 point (4) des rappels, 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 8 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, comme $\Phi_n(X^a) = \prod_{d|a} \Phi_{nd}(X)$ si $a, n \geq 1$ sont des entiers premiers entre eux, on a

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

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

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

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

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

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