DOMAINE : Arithmétique
NIVEAU : Avancé
CONTENU : Cours et exercices

AUTEUR : Margaret BILU
STAGE : Montpellier 2012

Polynômes cyclotomiques

- Polynômes cyclotomiques -

L'essentiel de ce cours provient de l'article *Elementary Properties of Cyclotomic Polynomials* de Yimin Ge.

Définition : Soit $n \in \mathbb{N}^*$. Une racine n-ième de l'unité est un nombre complexe ζ tel que $\zeta^n = 1$ (autrement dit, une racine complexe du polynôme $X^n - 1$). On dit que c'est une racine primitive n-ième si de plus $\zeta^k \neq 1$ pour $k = 1, \dots n-1$. Le plus petit $k \geqslant 1$ tel que $\zeta^k = 1$ est appelé l'ordre de ζ, et noté $\mathrm{ord}(\zeta)$.

Les racines n-ièmes de l'unité sont exactement les nombres complexes $e^{\frac{2ik\pi}{n}}$, $k = 0, \dots, n-1$. Les racines primitives sont celles de la forme $e^{\frac{2i\pi k}{n}}$, avec k premier avec n. En particulier, il y a exactement $\varphi(n)$ racines primitives n-ièmes.

Définition : Soit n un entier strictement positif. Alors le n-ième polynôme cyclotomique, noté Φ_n, est le polynôme unitaire qui a pour racines exactement les racines primitives n-ièmes, c'est-à-dire

$$\Phi_n(X) = \prod_{\substack{\zeta^n=1 \\ \mathrm{ord}(\zeta)=n}} (X - \zeta).$$

Remarque : Dans le cas particulier où $n = p$ est premier, toutes les racines p-ièmes différentes de 1 sont primitives, et donc

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

Proposition : Soit n un entier strictement positif. Alors

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{1}$$

Démonstration. $X^n - 1$ n'a que des racines simples qui sont exactement les racines n-ièmes de l'unité. D'autre part, si ζ est une racine n-ième de l'unité et $d = \mathrm{ord}(\zeta)$, alors ζ est une racine de Φ_d, et comme $d|n$, ζ est une racine du côté droit. Ainsi le côté et le côté gauche ont les mêmes racines, qui sont simples des deux côtés. Puisqu'ils sont unitaires, ils sont égaux.

Remarque : Si on compare les degrés de ces polynômes, on retrouve l'identité bien connue

$$n = \sum_{d|n} \varphi(d).$$

Lemme : Soient f et g des polynômes unitaires à coefficients rationnels. Si fg a des coefficients entiers, alors f et g sont en fait à coefficients entiers.

Démonstration. On écrit $f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_0$ et $g(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_0$, et on note $M > 0$ le plus petit dénominateur commun des a_i, $N > 0$ le plus petit dénominateur commun des b_i. Alors

$$Mf(X) = A_m X^m + \ldots + A_1 X + A_0$$

avec des entiers A_i premiers entre eux dans leur ensemble, et

$$Ng(X) = B_n X^n + \ldots + B_1 X + B_0$$

avec des entiers B_j premiers entre eux dans leur ensemble. De plus,

$$MNfg(X) = A_m B_n X^{m+n} + \ldots + (A_1 B_0 + B_1 A_0)X + A_0 B_0$$

a des coefficients entiers divisibles par MN, en utilisant le fait que fg est à coefficients entiers. Supposons que $MN \neq 1$, et soit dans ce cas un diviseur premier p de MN. Il existe alors i, j tels que p ne divise pas A_i et p ne divise pas B_j. On note I, J les plus grands i et j vérifiant cela. Le coefficient devant X^{I+J} dans $MNf(X)g(X)$ est alors congru à $A_I B_J$ modulo p, ce qui contredit le fait qu'il soit divisible par MN.

Proposition : Soit n un entier strictement positif. Alors Φ_n est un polynôme à coefficients entiers.

Démonstration. On raisonne par récurrence forte sur n. Le cas $n = 1$ est clair puisque $\Phi_1 = X - 1$. Supposons que Φ_k est à coefficients entiers pour tout $k < n$. Alors $X^n - 1 = \Phi_n(X)g_n(X)$ où $g_n(X) = \prod_{d|n,\, d<n} \Phi_d$ est à coefficients entiers par hypothèse de récurrence, donc $\Phi_n(X)$ est à coefficients rationnels, et le lemme précédent permet de conclure.

La formule (1) peut, grâce à un outil appelé inversion de Möbius, nous donner une formule « explicite »pour les polynômes cyclotomiques.

- Inversion de Möbius -

Définition : Le fonction de Möbius $\mu : \mathbb{N} \longrightarrow \{-1, 0, 1\}$ est définie de la manière suivante :

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

Proposition Soit $n \in \mathbb{N}^*$. Alors

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

Démonstration. Le cas $n = 1$ étant clair, supposons $n \geqslant 2$. On pose

$$m = \prod_{\substack{p \text{ premier} \\ p|n}} p$$

le produit de tous les nombres premiers distincts divisant n. Alors par définition de μ, on peut éliminer les diviseurs de n qui sont divisibles par un carré, et on a

$$\sum_{d|n} \mu(d) = \sum_{d|m} \mu(d).$$

Soit p un facteur premier de m (il y en a au moins un car $n \geqslant 2$). Alors

$$\sum_{d|m} \mu(d) = \sum_{d|\frac{m}{p}} (\mu(d) + \mu(pd)) = \sum_{d|\frac{m}{p}} (\mu(d) - \mu(d)) = 0.$$

Théorème : (Inversion de Möbius) Soient $F, f : \mathbb{N} \longrightarrow \mathbb{N}$ deux fonctions telles que

$$F(n) = \sum_{d|n} f(d).$$

Alors

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right).$$

Démonstration. Il est clair que les deux formules proposées sont les mêmes, donc il suffit de montrer la première. Or on a, en remplaçant F par son expression en fonction de f,

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{t|\frac{n}{d}} f(t) = \sum_{t|n} f(t) \sum_{d|\frac{n}{t}} \mu(d).$$

La proposition précédente nous dit que $\sum_{d|\frac{n}{t}} \mu(d)$ est non-nul si et seulement si $n = t$, et égal à 1 dans ce cas-là, d'où le résultat.

L'inversion de Möbius existe aussi sous forme multiplicative, la preuve étant la même en remplaçant les sommes par des produits.

Théorème : (Inversion de Möbius multiplicative) Soient $F, f : \mathbb{N} \longrightarrow \mathbb{N}$ deux fonctions telles que

$$F(n) = \prod_{d|n} f(d).$$

Alors

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

Exemple Appliquant l'inversion de Möbius à $F = \mathrm{id}$ et $f = \varphi$ la fonction indicatrice d'Euler, reliées par la relation

$$n = \sum_{d|n} \varphi(d),$$

on obtient

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = \sum_{d|n} d\mu\left(\frac{n}{d}\right).$$

Si par exemple $n = p^k$, on retrouve bien $\varphi(p^k) = p^k - p^{k-1}$.

De même, appliquant l'inversion de Möbius multiplicative à la formule (1) prise pour $\varphi(n)+1$ valeurs entières distinctes de X et en utilisant un polynôme interpolateur de Lagrange, on trouve la formule suivante pour les polynômes cyclotomiques :

Théorème : Soit n un entier strictement positif. Alors

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

Grâce à cette expression, on peut prouver le résultat suivant, qui permet de relier deux polynômes cyclotomiques dont les indices se divisent l'un l'autre :

Proposition : Soit $n \in \mathbb{N}^*$ et p un nombre premier. Alors

$$\Phi_{pn}(X) = \begin{cases} \Phi_n(X^p) & \text{si } p|n \\ \frac{\Phi_n(X^p)}{\Phi_n(X)} & \text{sinon.} \end{cases}$$

Démonstration. On a

$$\begin{aligned} \Phi_{pn}(X) &= \prod_{d|pn} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)} \\ &= \prod_{d|n} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)} \prod_{\substack{d|pn \\ d\nmid n}} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)} \end{aligned}$$

.

Si $p|n$, alors $d|pn$ et $d \nmid n$ impliquent que $p^2|d$, donc $\mu(d) = 0$ et on a bien $\Phi_{pn}(X) = \Phi_n(X^p)$ dans ce cas. Si maintenant $p \nmid n$, alors

$$\begin{aligned} \Phi_n(X) &= \prod_{d|n} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)} \prod_{d|n} \left(X^{\frac{pn}{pd}} - 1\right)^{\mu(pd)} \\ &= \prod_{d|n} \left(X^{\frac{pn}{d}} - 1\right)^{\mu(d)} \prod_{d|n} \left(X^{\frac{n}{d}} - 1\right)^{-\mu(d)} \\ &= \frac{\Phi_n(X^p)}{\Phi_n(X)}. \end{aligned}$$

Remarque : En particulier, on retrouve bien, pour p premier, $\Phi_p(X) = \frac{\Phi_1(X^p)}{\Phi_1(X)} = \frac{X^p-1}{X-1}$.

Le corollaire suivant est alors immédiat :

Corollaire Soit p premier et $n, k \in \mathbb{N}^*$. Alors

$$\Phi_{p^k n}(X) = \begin{cases} \Phi_n(X^{p^k}) & \text{si } p|n \\ \frac{\Phi_n(X^{p^k})}{\Phi_n(X^{p^{k-1}})} & \text{sinon.} \end{cases}$$

- Diviseurs premiers des valeurs entières prises par un polynôme cyclotomique -

Nous savons que les polynômes cyclotomiques sont à coefficients entiers, donc nous allons pouvoir les étudier modulo des entiers. En particulier, nous allons classifier les diviseurs premiers de $\Phi_n(x)$ pour $n \geqslant 1$ et x entiers.

Lemme : Soit p un nombre premier. Si $X^n - 1$ a une racine double modulo p, alors $p|n$.

Démonstration. Par hypothèse, $X^n - 1 \pmod p$ a un pgcd de degré supérieur à 1 avec sa dérivée nX^{n-1}, ce qui est possible seulement si cette dernière est nulle, c'est-à-dire si $p|n$.

Proposition : Soit $n \in \mathbb{N}^*$, d un diviseur strict de n et x un entier. Si $\Phi_n(x)$ et $\Phi_d(x)$ ont un diviseur premier commun p, alors $p|n$.

Démonstration On a $x^n - 1 = \prod_{t|n} \Phi_t(x)$ d'après la formule (1). Ainsi, $X^n - 1$ a une racine double modulo p en $X = x$, et par le lemme précédent, $p|n$.

Nous arrivons à un résultat clé du cours, qui est celui qui va servir dans la plupart des applications :

Théorème : (Résultat fondamental) Soit $n \in \mathbb{N}^*$, $x \in \mathbb{Z}$. Alors tout diviseur premier p de $\Phi_n(x)$ vérifie

– $p \equiv 1 \pmod n$ si x est d'ordre n modulo p

– $p|n$ sinon.

Démonstration. Soit p un diviseur premier de $\Phi_n(x)$. x est premier avec p car $p|\Phi_n(x)|x^n - 1$, et on peut donc poser $k = \mathrm{ord}_p(a)$ (qui divise n).

Si $k = n$, alors $p \equiv 1 \pmod n$ par le petit théorème de Fermat.

Sinon, $0 \equiv x^k - 1 \equiv \prod_{d|k} \Phi_d(x) \pmod p$, donc il existe un diviseur d de k tel que $p|\Phi_d(x)$. Mais $d|k|n$ et $d < n$, donc donc d'après la proposition précédente, $p|n$.

Un autre résultat qui peut être utile est le suivant :

Proposition : Soient a et b des entiers positifs. S'il existe un entier x tel que

$$\text{pgcd}(\Phi_a(x), \Phi_b(x)) > 1$$

alors $\frac{a}{b}$ est une puissance de p.

Démonstration. Supposons que p est un diviseur premier commun de $\Phi_a(x)$ et de $\Phi_b(x)$. Nous allons montrer que $\frac{a}{b}$ est une puissance de p. Pour cela, écrivons $a = p^\alpha A$, $b = p^\beta B$ avec A, B non divisibles par p et montrons que $A = B$.

Première étape : Nous allons montrer que $p|\Phi_A(x)$. C'est évident pour $\alpha = 0$. Si $\alpha > 1$, on a vu que, A étant premier avec p,

$$\Phi_a(X) = \frac{\Phi_A(X^{p^\alpha})}{\Phi_A(X^{p^{\alpha-1}})},$$

et donc

$$0 \equiv \Phi_a(x) \equiv \frac{\Phi_A(x^{p^\alpha})}{\Phi_A(x^{p^{\alpha-1}})} \pmod{p},$$

ce qui implique que $\Phi_A(x^{p^\alpha}) \equiv 0 \pmod{p}$. D'autre part, si on itère $x^p \equiv x \pmod{p}$, on obtient que $x^{p^\alpha} \equiv x \pmod{p}$, d'où $\Phi_A(x) \equiv \Phi_A(x^{p^\alpha}) \equiv 0 \pmod{p}$. De même, on a $p|\Phi_B(x)$.

Deuxième étape : Puisque p divise $\Phi_a(x)$ et $\Phi_b(x)$, il divise $x^a - 1$ et $x^b - 1$, donc il divise $\text{pgcd}(x^a - 1, x^b - 1) = |x^{\text{pgcd}(a,b)} - 1|$. Posons $k = \text{pgcd}(A, B)$ et supposons que $A \neq B$. Alors k est strictement inférieur à au moins l'un des entiers A et B, disons A. On a

$$0 \equiv x^k - 1 \equiv \prod_{d|k} \Phi_d(x) \pmod{p},$$

donc il existe un diviseur d de k, qui est un diviseur strict de A, tel que $p|\Phi_d(x)$. Par la propriété précédant le résultat fondamental, on en conclut $p|A$, qui est une contradiction. Donc $A = B$.

- Applications et exercices -

Le résultat que nous venons de voir permet de prouver un cas particulier du théorème de Dirichlet sur les nombres premiers dans les progressions arithmétiques :

Théorème : (Dirichlet) Soit $n \in \mathbb{N}^*$. Alors il existe une infinité de nombres premiers p congrus à 1 modulo n.

Démonstration Le cas $n = 1$ correspond à l'infinité des nombres premiers tout court, donc est clair. Nous pouvons cependant nous en inspirer pour la preuve du cas $n \geqslant 2$. En effet, la preuve de l'infinité des nombres premiers consiste à supposer qu'il n'y a qu'un nombre fini $p_1, \ldots, p_k$ de nombres premiers, et d'évaluer le polynôme $X + 1$ en $p_1 \ldots p_k$ pour obtenir une contradiction. L'idée ici est la même : supposons qu'il n'y a qu'un nombre fini $p_1 \ldots p_k$ de nombres premiers congrus à 1 modulo n. On pose

$$m = p_1 \ldots p_k \prod_{\substack{p \mid n \\ p \text{ premier}}} p.$$

Le produit à utiliser est un peu plus complexe car il faut aussi éliminer les facteurs premiers de n. Etant donné que $n \geqslant 2$, on a $m > 1$. Le polynôme à utiliser va être Φ_n : puisque c'est un polynôme unitaire non-constant, il existe un entier k tel que $\Phi_n(m^k) > 1$. Soit alors q un diviseur premier de $\Phi_n(m^k)$. q divise $m^{kn} - 1$, donc q est premier avec m. Ainsi, q n'est pas parmi les p_i, donc n'est pas congru à 1 modulo n, et ne divise pas n. Ceci est une contradiction avec notre résultat fondamental.

Exercice 1 (IMO Shortlist 2006) Trouver toutes les solutions entières de l'équation

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

Exercice 2 Soit $a > 1$ un entier fixé. Montrer que $\frac{p-1}{\mathrm{ord}_p(a)}$ est non borné lorsque p parcourt l'ensemble des nombres premiers.

Exercice 3 (IMO Shortlist 2002, généralisation) Soient $p_1, \ldots, p_n$ des nombres premiers impairs. Montrer que $2^{p_1 p_2 \cdots p_n} + 1$ a au moins $2^{2^{n-1}}$ diviseurs.

- Solution des exercices -

Solution de l'exercice 1 L'équation équivaut à

$$\Phi_7(x) = (y - 1)(1 + \ldots + y^4).$$

Remarquons que le côté gauche est toujours strictement positif, et que donc y doit être supérieur à 2. Le résultat fondamental nous dit que tout diviseur

premier du côté gauche soit est égal à 7, soit est congru à 1 modulo 7. Ainsi, tout diviseur positif du côté gauche est soit divisible par 7, soit congru à 1 modulo 7. $y - 1$ étant un tel diviseur, on a $y \equiv 1$ ou $2 \pmod 7$. Dans ce cas, $1 + y + \ldots + y^4 \equiv 5$ ou $3 \pmod 7$, ce qui est une contradiction car il devrait aussi être congru à 0 ou 1 modulo 7. L'équation n'a donc pas de solutions.

Solution de l'exercice 2 La solution utilise le lemme suivant, qui a déjà un intérêt en soi :

Lemme Soit $n \in \mathbb{N}^*$. Il existe un nombre premier $p > a$ tel que les n entiers

$$p + 1, 2p + 1, \ldots, np + 1$$

ne sont pas premiers.

Démonstration. Choisissons $p_1, \ldots, p_n$ des nombres premiers distincts strictement plus grands que n, et considérons le système de congruences

$$\begin{cases} x + 1 \equiv 0 \pmod{p_1^2} \\ 2x + 1 \equiv 0 \pmod{p_2^2} \\ \vdots \\ nx + 1 \equiv 0 \pmod{p_n^2}, \end{cases}$$

qui, puisque $2, \ldots, n$, étant plus petits que les p_i, sont inversibles modulo les p_i, est equivalent au système

$$\begin{cases} x \equiv -1 \pmod{p_1^2} \\ x \equiv -\frac{1}{2} \pmod{p_2^2} \\ \vdots \\ x \equiv -\frac{1}{n} \pmod{p_n^2}. \end{cases}$$

Soit x_0 une solution de ce système, obtenue grâce au lemme chinois. Alors tout nombre de la forme $x_0 + kp_1^2 \ldots p_n^2$ est aussi solution de ce système. D'après le théorème de Dirichlet, il existe un nombre premier $p > a$ de cette forme-là. Alors $p + 1, \ldots, np + 1$ ne sont pas premiers, étant chacun divisible par un carré.

Revenons maintenant à l'exercice. Soit p comme dans le lemme, et q un diviseur premier de $\Phi_p(a)$. Si on avait $q|p$, on aurait $q = p$, donc $a^q \equiv 1 \pmod q$, donc $a \equiv 1 \pmod q$, ce qui est impossible car $a < p = q$. Donc par le résultat fondamental, $q \equiv 1 \pmod p$ et $\mathrm{ord}_q(a) = p$. Or, $p + 1, \ldots, np + 1$

étant composés, $q \geqslant (n+1)p+1$, donc $\frac{q-1}{\mathrm{ord}_q(a)} \geqslant n+1$, ce qui conclut, puisque n était arbitraire.

Solution de l'exercice 3 Il suffit de montrer que $2^{p_1 \dots p_n}+1$ a au moins 2^{n-1} diviseurs premiers deux à deux. On écrit

$$\begin{aligned}
(2^{p_1 \dots p_n}-1)(2^{p_1 \dots p_n}+1) &= 2^{2p_1 \dots p_n}-1 \\
&= \prod_{d \mid 2p_1 \dots p_n} \Phi_d(2) \\
&= \left(\prod_{d \mid p_1 \dots p_n} \Phi_d(2) \right) \left(\prod_{d \mid p_1 \dots p_n} \Phi_{2d}(2) \right) \\
&= (2^{p_1 \dots p_n}-1) \left(\prod_{d \mid p_1 \dots p_n} \Phi_{2d}(2) \right),
\end{aligned}$$

d'où

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

Par la proposition qui suit le résultat fondamental, nous savons que si $\Phi_a(2)$ et $\Phi_b(2)$ ne sont pas premiers entre eux, alors $\frac{a}{b}$ doit être une puissance d'un nombre premier. Il suffit donc que nous prouvions que nous pouvons choisir 2^{n-1} diviseurs de $p_1 \dots p_n$ tels que deux d'entre eux ne diffèrent jamais d'un seul nombre premier. On effectue cela en choisissant les diviseurs qui sont produit d'exactement un nombre pair de facteurs premiers : il y en a bien 2^{n-1}, d'où le résultat.