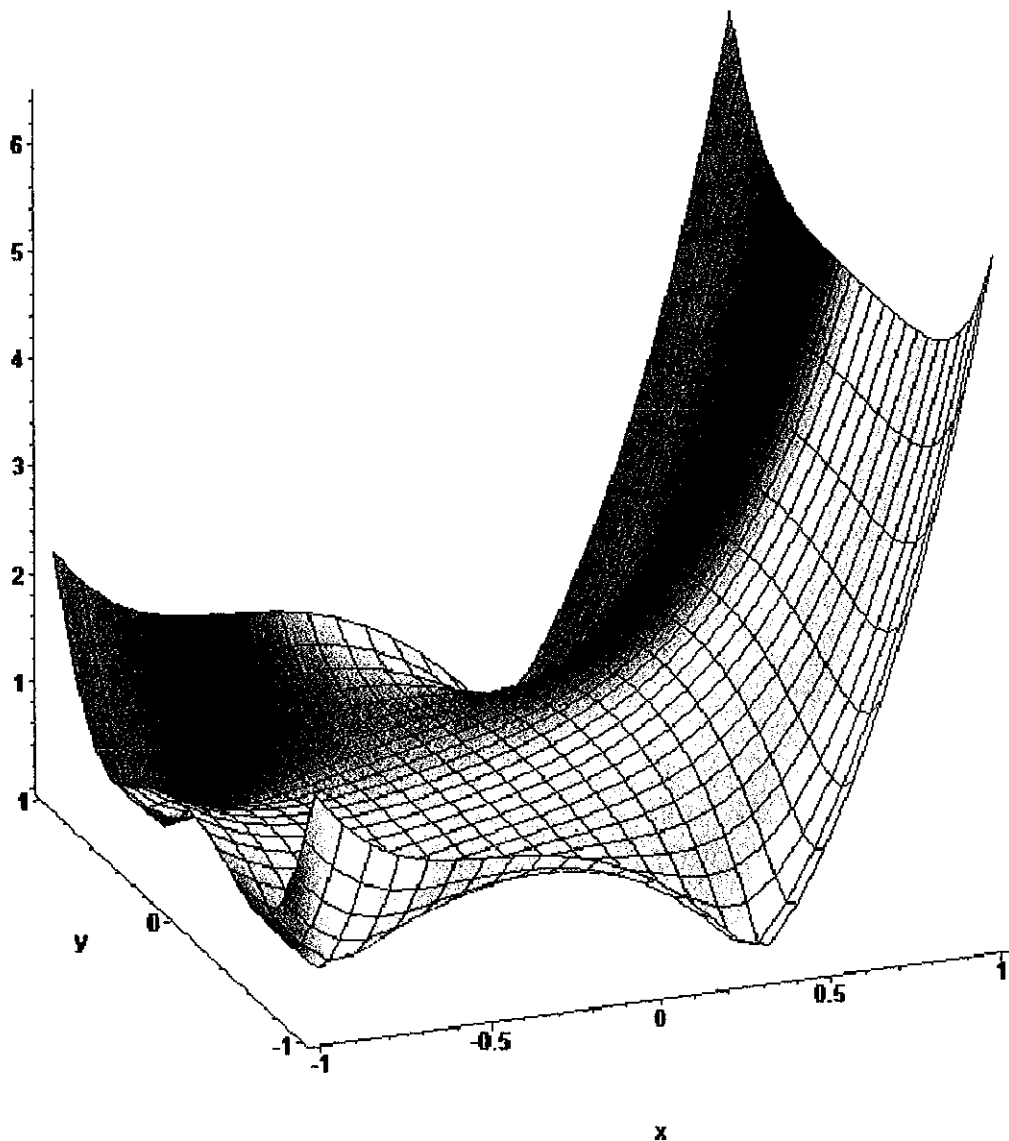


Polynômes cyclotomiques



Représentation 3D du polynôme cyclotomique complexe $\Phi_5(X)$

Préliminaires

Fonction indicatrice d'Euler φ

1. Définition

La fonction indicatrice d'Euler est la fonction :

$$n \in \mathbb{N}^* \mapsto \varphi(n) = |\{k \text{ entier} / 1 \leq k \leq n \text{ et } k \wedge n = 1\}|$$

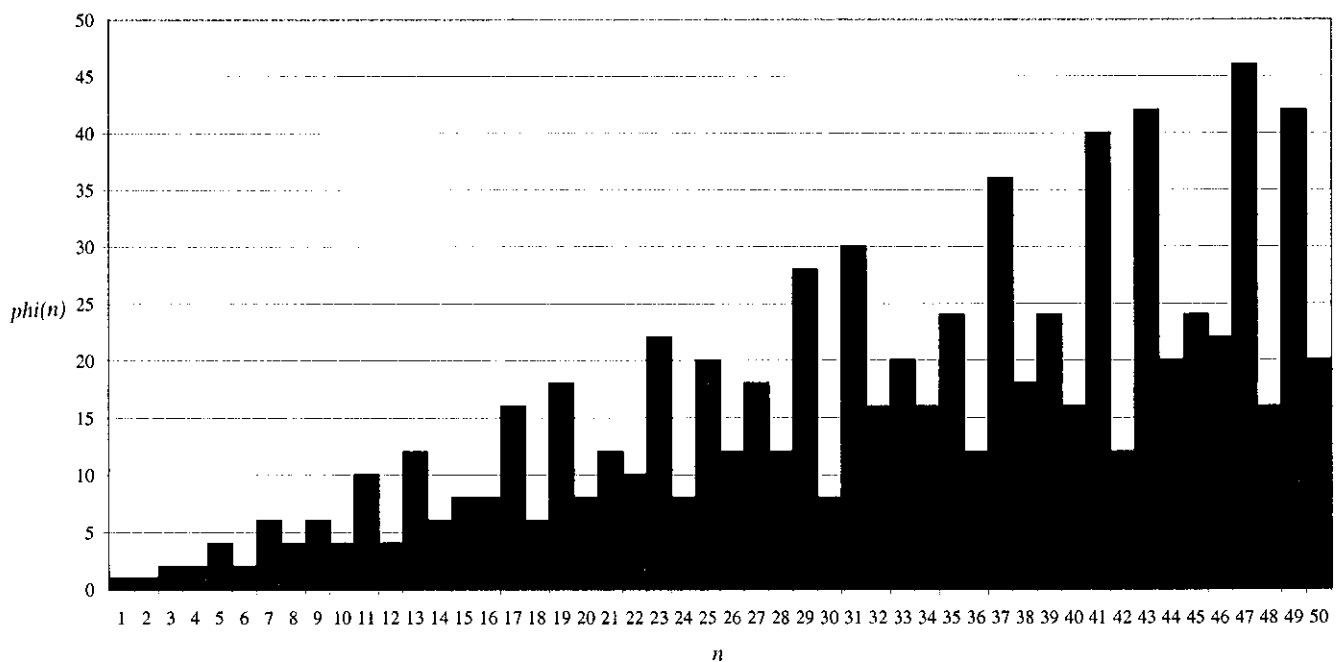
$\varphi(n)$ peut être aussi défini comme :

- ✓ le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$,
- ✓ le nombre d'éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, \times)$
- ✓ le nombre de racines $n^{\text{ième}}$ primitives de l'unité dans \mathbb{C} .

Exemples :

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\varphi(i)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Fonction indicatrice d'Euler



2. Propriétés immédiates :

1. $\varphi(1) = 1$.
2. Si p est premier, $\varphi(p) = p - 1$.
3. Si $n = p^r$ où p est premier, $\varphi(n) = p^r - p^{r-1} = p^{r-1}(p - 1)$.
4. La fonction φ est multiplicative : si m et n premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$.

5. Si la décomposition de $n > 1$ en facteurs premiers est : $n = \prod_{i=1}^k p_i^{\alpha_i}$, alors :

$$\varphi(n) = \prod_{i=1}^k p_i^{\alpha_i-1} (p_i - 1) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

6. Si $n > 2$, $\varphi(n)$ est pair.

DEMONSTRATION :

1. Évident.
2. Évident.
3. Si $n = p^r$, les seuls éléments non premiers avec n de $1 \cdots p^r$ sont les éléments de la forme $k p$ où $1 \leq k \leq p^{r-1}$ et leur nombre est p^{r-1} .
4. Résulte de l'isomorphisme entre $(\mathbb{Z}/n\mathbb{Z}, +) \times (\mathbb{Z}/m\mathbb{Z}, +)$ et $(\mathbb{Z}/mn\mathbb{Z}, +)$ lorsque m et n sont premiers entre eux.
5. Résulte de 2 et 3.
6. Si $n = 2^r$, avec $1 < r$, $\varphi(n) = 2^{r-1}(2-1)$ est pair. Sinon n comprend au moins un facteur premier impair p et $\varphi(n)$ est un multiple de $p-1$.

3. Proposition

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

DEMONSTRATION :

Soit l'ensemble des n fractions : $F = \left\{ \frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n} \right\}$. Après mise sous forme irréductible ces fractions, on définit, pour chaque diviseur d de n , $F_d = \left\{ \frac{k}{d} \in F / 1 \leq k \leq d \text{ et } k \wedge d = 1 \right\}$.

Il est clair alors que :

- ✓ L'ensemble des F_d avec $d|n$ est une partition de F .
- ✓ $|F_d| = \varphi(d)$.

D'où la formule.

4. Théorème d'Euler

Soit $n, a \in \mathbb{N}^*$ premiers entre eux, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Si n est premier $a^n \equiv a \pmod{n}$ (petit théorème de Fermat)

DEMONSTRATION :

Un élément a de $(\mathbb{Z}/n\mathbb{Z}, \times)$ est inversible si et seulement si il est premier avec n . En notant $U(\mathbb{Z}/n\mathbb{Z}, \times)$ le groupe multiplicatif formé par les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, \times)$, on a donc : $|U(\mathbb{Z}/n\mathbb{Z}, \times)| = \varphi(n)$.

Comme $a \in U(\mathbb{Z}/n\mathbb{Z}, \times)$, son ordre, c'est-à-dire le plus petit entier k tel que $a^k = 1$ est, selon le théorème de Lagrange, un diviseur de l'ordre de l'ordre $\varphi(n)$ de $U(\mathbb{Z}/n\mathbb{Z}, \times)$. D'où : $a^{\varphi(n)} \equiv 1$ dans $(\mathbb{Z}/n\mathbb{Z}, \times)$.

Si n est premier $\varphi(n) = n-1$. Si a est un multiple de n , alors $a \equiv 0 \pmod{n}$ et la formule est vraie. Si a n'est pas multiple de n , le résultat précédent s'applique pour aboutir à la même formule.

Fonction de Mobius μ

5. Définition

La fonction de Mobius $\mathbb{N}^* \xrightarrow{\mu} \mathbb{Z}$ est définie par :

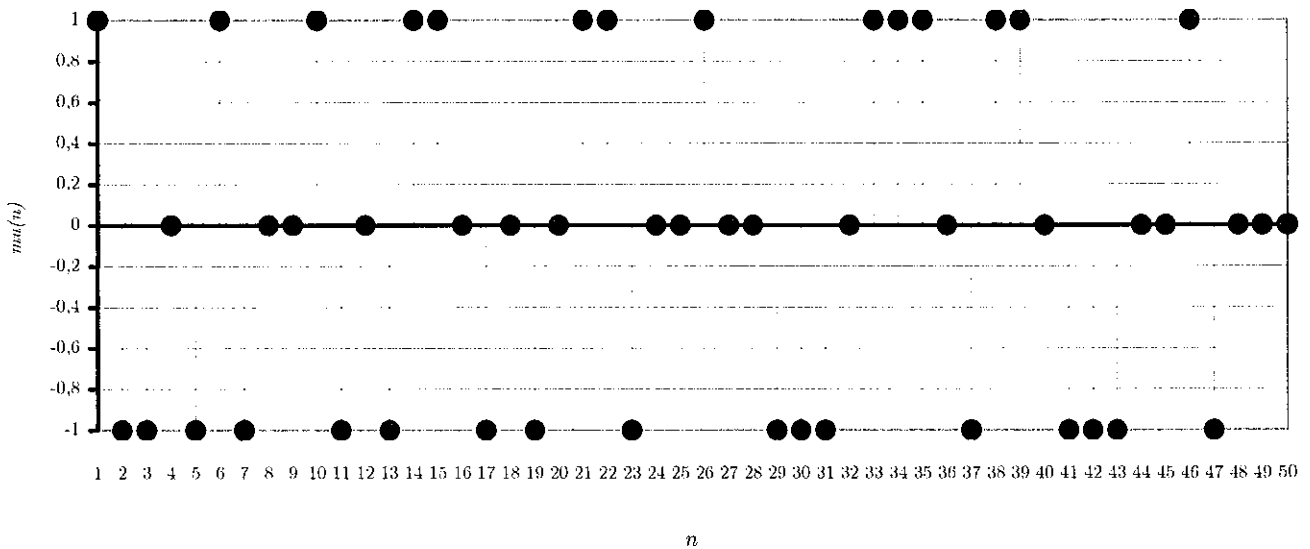
Soit la décomposition de n en facteurs premiers est : $n = \prod_{i=1}^k p_i^{\alpha_i}$

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ a un facteur premier carré autrement dit si il existe } \alpha_i \geq 2 \\ (-1)^r & \text{si } n \text{ a } r \text{ facteurs premiers (d'exposant 1)} \end{cases}$$

Exemples :

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\mu(i)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1	1	0	-1	0	-1	0

Fonction mu de Mobius



6. Propriétés immédiates

1. La fonction μ est multiplicative : si m et n premiers entre eux, $\mu(mn) = \mu(m)\mu(n)$.
2. Si $n > 1$, $\sum_{d|n} \mu(d) = 0$.

DEMONSTRATION :

1.
 - ✓ Si $n = 1$ ou $m = 1$, c'est évident.
 - ✓ Si m ou n ont un facteur carré, alors $\mu(m)\mu(n) = 0$. Alors, mn a aussi un facteur carré. Donc $\mu(mn) = 0$
 - ✓ Dans le dernier cas $m = p_1 \cdots p_r$, et $n = q_1 \cdots q_s$. Et $\mu(m) = (-1)^r$, $\mu(n) = (-1)^s$ Comme m et n sont premiers entre eux leurs facteurs sont distincts et la décomposition de mn en facteurs premiers est : $mn = p_1 \cdots p_r q_1 \cdots q_s$. D'où : $\mu(m)\mu(n) = (-1)^r (-1)^s = (-1)^{r+s} = \mu(mn)$.

2.

Soit $n = \prod_{i=1}^k p_i^{\alpha_i}$ et $m = \prod_{i=1}^k p_i$. On a alors : $\sum_{d|n} \mu(d) = \sum_{d|m} \mu(d)$, car tout diviseur de n ne divisant pas m a un facteur carré et son image par μ est nulle. Pour $0 \leq i \leq k$, on a C_k^i diviseurs d formés de i facteurs choisis parmi les k facteurs de m (on compte le diviseur 1 comme ayant 0 facteur). D'où :

$$\sum_{d|m} \mu(d) = \sum_{i=0}^k C_k^i \mu(i) = \sum_{i=0}^k C_k^i (-1)^i = (1-1)^k = 0$$

7. Lemme

Soit $n \in \mathbb{N}^*$ et $A_n = \{(a,b) / a,b \in \mathbb{N}^*, a|n \text{ et } b|a\}$ et $B_n = \{(xy,x) / x,y \in \mathbb{N}^*, x|n \text{ et } y|\frac{n}{x}\}$, alors $A = B$.

DEMONSTRATION :

1. Soit $(a,b) \in A_n$. Comme $b|a$ on peut poser $x = \frac{a}{b}$ et $y = b$. Comme $b|a$ et $a|n$, $b|\frac{n}{x}$. On a donc $(a,b) = (xy,x)$ avec $x|n$ et $n = kxy \Rightarrow \frac{n}{x} = ky \Rightarrow y|\frac{n}{x}$. Donc $(a,b) = (xy,x) \in B_n$.
2. Soit $(xy,x) \in B_n$. En posant $b = x$, et $a = xy$, on a : $b|a$ et $y|\frac{n}{x} \Rightarrow \frac{n}{x} = ky \Rightarrow n = kxy \Rightarrow a|\frac{n}{y}$. Et $(a,b) = (xy,x) \in A_n$.

8. Proposition : formule d'inversion de Mobius

Soit un couple de fonctions f, g de $\mathbb{N}^* \rightarrow G$ groupe abélien, alors :

Si G est noté additivement :

$$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{a|n} \mu\left(\frac{n}{a}\right) g(a)$$

Si G est noté multiplicativement :

$$g(n) = \prod_{d|n} f(d) \iff f(n) = \prod_{a|n} g(a)^{\mu\left(\frac{n}{a}\right)}$$

DEMONSTRATION :

Remarques préliminaires :

- ✓ Comme $\mu(a) \in \{-1, 0, 1\}$ les expressions de droite ont un sens.
- ✓ $\sum_{a|n} \mu\left(\frac{n}{a}\right) g(a) = \sum_{a|n} \mu(a) g\left(\frac{n}{a}\right)$, puisque $a|n \iff \frac{n}{a}|n$.
- ✓ La démonstration va être faite pour la forme additive avec notations et résultat du lemme 7.

Soit $g(n) = \sum_{d|n} f(d)$

$$\sum_{a|n} \mu\left(\frac{n}{a}\right) g(a) = \sum_{a|n} \mu\left(\frac{n}{a}\right) \underbrace{\left(\sum_{b|a} f(b)\right)}_{=g(a)} = \sum_{(a,b) \in A_n} \mu\left(\frac{n}{a}\right) f(b)$$

Selon le lemme 7 :

$$\sum_{a|n} \mu\left(\frac{n}{a}\right) g(a) = \sum_{(a,b) \in A_n} \mu\left(\frac{n}{a}\right) f(b) = \sum_{(xy,x) \in B_n} \mu\left(\frac{n}{xy}\right) f(x) = \sum_{x|n} \sum_{y|\frac{n}{x}} \mu\left(\frac{n}{xy}\right) f(x) = \sum_{x|n} f(x) \sum_{y|\frac{n}{x}} \mu\left(\frac{n}{xy}\right)$$

Or, selon 6, $\sum_{y|\frac{n}{x}} \mu\left(\frac{n}{xy}\right) = \begin{cases} 1 & \text{si } \frac{n}{x} = 1 \\ 0 & \text{sinon} \end{cases}$ D'où : $\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = f(n)$.

La réciproque se démontre de façon analogue.

9. Corollaire

$$n = \sum_{d|n} \varphi(d) \Leftrightarrow \varphi(n) = \sum_{d|n} \mu(d) \frac{d}{n}$$

Polynômes cyclotomiques :

définition, premières propriétés

Dans la suite, pour $n \in \mathbb{N}^*$ on désignera par \mathcal{P}_n l'ensemble des $\varphi(n)$ racines n^{me} primitives de l'unité dans \mathbb{C} et par ω un élément quelconque de \mathcal{P}_n , par exemple $\omega = e^{\frac{2i\pi}{n}}$.

10. Définition

Le polynôme cyclotomique d'ordre n $\Phi_n(X) \in \mathbb{C}[X]$ est défini par :

$$\Phi_n(X) = \prod_{\omega \in \mathcal{P}_n} (X - \omega) = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} (X - \omega^k)$$

Exemples :

La fonction `cyclotomic(n, X)` du package `numtheory` de Maple retourne le polynôme cyclotomique d'ordre n $\Phi_n(X)$:

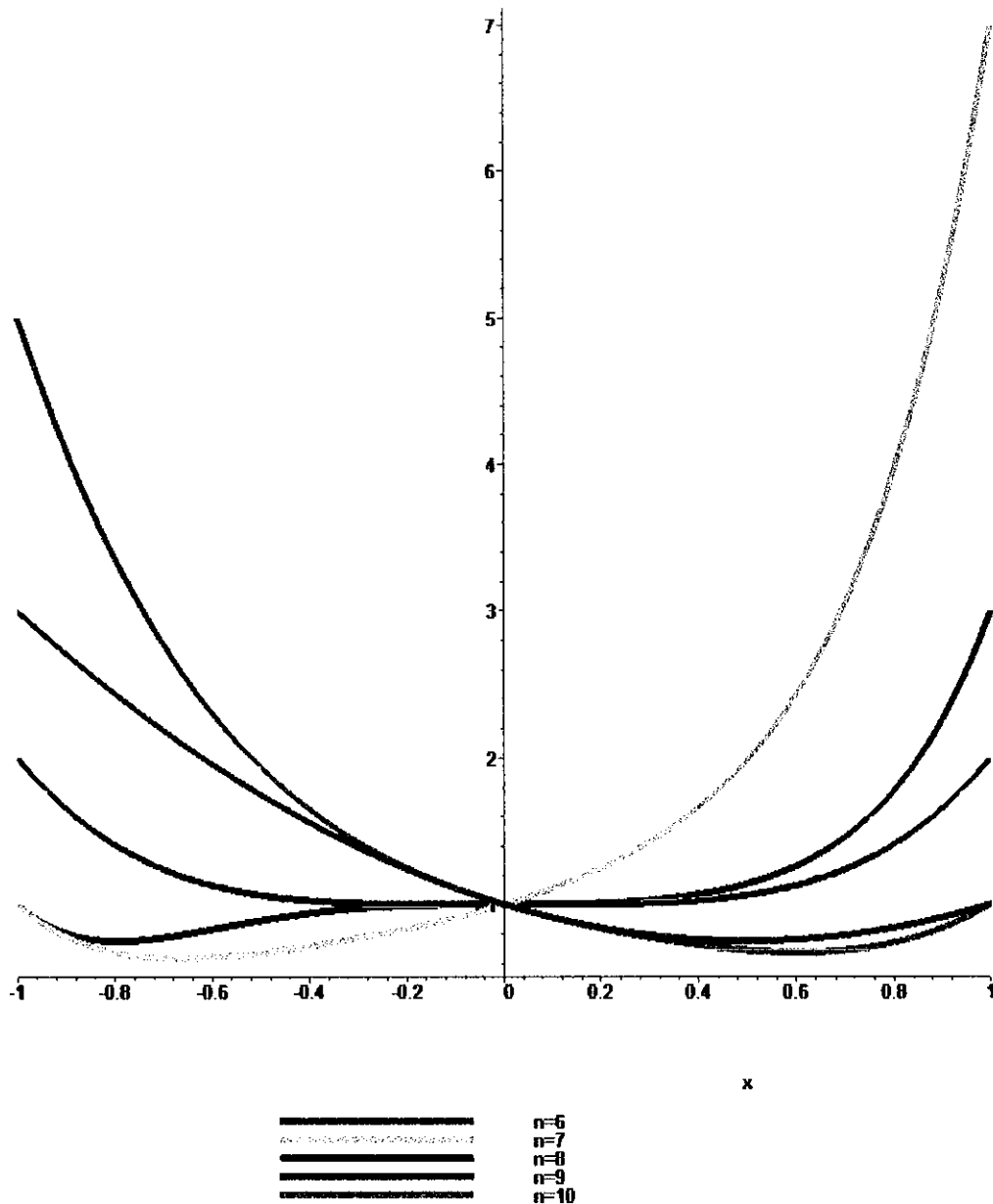
```
> for i from 1 to 16 do print(i, sort(cyclotomic(i, X))); od;
1, X - 1
2, X + 1
3, X^2 + X + 1
4, X^2 + 1
5, X^4 + X^3 + X^2 + X + 1
6, X^2 - X + 1
7, X^6 + X^5 + X^4 + X^3 + X^2 + X + 1
8, X^4 + 1
9, X^6 + X^3 + 1
10, X^4 - X^3 + X^2 - X + 1
11, X^10 + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1
12, X^4 - X^2 + 1
13, X^12 + X^11 + X^10 + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1
14, X^6 - X^5 + X^4 - X^3 + X^2 - X + 1
15, X^8 - X^7 + X^5 - X^4 + X^3 - X + 1
16, X^8 + 1
```

(le `sort` est destiné à obtenir les polynômes ordonnés selon les puissances décroissantes)

Surprise ! Tous les coefficients sur ces premiers exemples sont égaux à -1, 0 ou 1. Mais :

```
> sort(cyclotomic(105, X));
X^48 + X^47 + X^46 - X^43 - X^42 - 2 X^41 - X^40 - X^39 + X^36 + X^35 + X^34 + X^33
+ X^32 + X^31 - X^28 - X^26 - X^24 - X^22 - X^20 + X^17 + X^16 + X^15 + X^14 + X^13
+ X^12 - X^9 - X^8 - 2 X^7 - X^6 - X^5 + X^2 + X + 1
```

a deux coefficients égal à -2.



Courbes de $x \mapsto \Phi_n(x)$, $x \in [-1 \dots 1]$, $n \in 6 \dots 10$

11. Propriétés immédiates

1. $\Phi_n(X)$ est de degré $\varphi(n)$ donc de degré pair si $n > 2$.
2. Le polynôme $\Phi_n(X)$ est un diviseur du polynôme $X^n - 1$.
3. $\Phi_n(X)$ a toutes ses racines simples.
4. $\Phi_n(X)$ est unitaire.
5. Si n est premier, $\Phi_n(X) = 1 + X + \dots + X^{n-1}$.

DEMONSTRATION :

1. $|\mathcal{P}_n| = \varphi(n)$ et, selon 2.6 ; pour $n > 2$, $\varphi(n)$ est pair.
2. $X^n - 1 = \prod_{1 \leq k \leq n} (X - \omega^k)$.
3. Évident.
4. Évident.

5. Évident.

6. Si n est premier, les entiers $k \leq n$ premiers avec n sont : $1, 2, \dots, n-1$ et :

$$\Phi_n(X) = (X - \omega) \cdots (X - \omega^{n-1}) = \frac{(X-1)(X-\omega) \cdots (X-\omega^{n-1})}{(X-1)} = \frac{X^n - 1}{(X-1)} = 1 + X + \cdots + X^{n-1}.$$

12. Théorème

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

DEMONSTRATION :

En reprenant la démonstration de la proposition 3, $F = \left\{ \frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n} \right\}$:

$$X^n - 1 = \prod_{1 \leq j \leq n} \left(X - e^{\frac{j2i\pi}{n}} \right) = \prod_{\substack{j \in F \\ n}} \left(X - e^{\frac{j2i\pi}{n}} \right).$$

Comme les $F_d = \left\{ \frac{k}{d} \in F \mid 1 \leq k \leq d \text{ et } k \wedge d = 1 \right\}$ où $d|n$ forment une partition de F ,

$$X^n - 1 = \prod_{d|n} \prod_{\frac{k}{d} \in F_d} \left(X - e^{\frac{k}{d}2i\pi} \right)$$

Or $\prod_{\frac{k}{d} \in F_d} \left(X - e^{\frac{k}{d}2i\pi} \right) = \Phi_d(X).$

13. Corollaire

Les coefficients de $\Phi_n(X)$ sont entiers, autrement dit $\Phi_n(X) \in \mathbb{Z}[X]$

DEMONSTRATION :

Récurrence sur n :

1. Vrai pour $\Phi_1(X)$ et $\Phi_2(X)$.
2. Supposons vrai pour tout $k \leq n-1$. La formule du théorème 13 peut s'écrire :

$$X^n - 1 = \Phi_n(X) \prod_{\substack{d|n \\ d < n}} \Phi_d(X) \Leftrightarrow \Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d < n}} \Phi_d(X)}$$

Et, selon l'hypothèse de récurrence, tous les $\Phi_d(X)$ avec $d < n$ sont à coefficient entiers.

14. Théorème

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

DEMONSTRATION :

Soit $\mathbb{N}^* \xrightarrow{g} \mathbb{C}(X)^*$ où $\mathbb{C}(X)^*$ désigne le groupe multiplicatif des fonctions rationnelles non nulles sur $n \mapsto g(n) = \Phi_n(X)$

©. En posant $f(n) = \prod_{d|n} g(d)$, on obtient : $f(n) = \prod_{d|n} \Phi_d(X) = X^n - 1$ d'après le théorème 11. La formule

d'inversion de Mobius version multiplicative donne alors :

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

Application :

$$\begin{aligned} \Phi_8(X) &= \prod_{d|8} (X^d - 1)^{\mu\left(\frac{8}{d}\right)} = (X - 1)^{\mu(8)} (X^2 - 1)^{\mu(4)} (X^4 - 1)^{\mu(2)} (X^8 - 1)^{\mu(1)} \\ &= (X - 1)^0 (X^2 - 1)^0 (X^4 - 1)^{-1} (X^8 - 1)^1 = \frac{(X^4)^2 - 1}{X^4 - 1} = X^4 + 1 \end{aligned}$$

La démonstration de la proposition suivante requière un petit lemme :

15. Lemme

Soit, pour $3 \leq n$, \mathcal{P}_n l'ensemble des $\varphi(n)$ racines $n^{\text{ème}}$ primitives de l'unité dans \mathbb{C} . Alors :

- ✓ $\omega \in \mathcal{P}_n \Leftrightarrow \bar{\omega} = \frac{1}{\omega} \in \mathcal{P}_n$.
- ✓ $\prod_{\omega \in \mathcal{P}_n} \omega = 1$.

DEMONSTRATION :

$$\omega = e^{\frac{k}{n}2i\pi} \in \mathcal{P}_n \Leftrightarrow k \wedge n = 1. \quad \bar{\omega} = e^{-\frac{k}{n}2i\pi}. \quad \text{Or } k \wedge n = 1 \Rightarrow (n-k) \wedge n = 1. \quad \text{Donc } \bar{\omega} \in \mathcal{P}_n.$$

Pour la deuxième assertion, il suffit de regrouper par couples $(\omega, \bar{\omega})$ les termes du produit $\prod_{\omega \in \mathcal{P}_n} \omega$ pour obtenir le résultat.

16. Proposition

Pour $n \geq 2$ $\Phi_n(X)$ est un polynôme palindromique. Autrement dit les coefficients a_j vérifient : $a_j = a_{\varphi(n)-j}$. En particulier $a_0 = \Phi_n(0) = a_{\varphi(n)} = 1$.

DEMONSTRATION :

Au préalable on peut remarquer que $\Phi_2(X) = X + 1$ est palindromique.

Pour un polynôme $P(X) = \sum_{j=0}^m a_j X^j$, le polynôme réciproque est $\tilde{P}(X) = \sum_{j=0}^m a_j X^{m-j}$

Dans $\mathbb{C}[X]$ où on peut assimiler polynômes et fonctions polynômes : $\tilde{P}(X) = X^m P(1/X)$.

$\Phi_n(X)$ est un polynôme palindromique équivaut donc à $\Phi_n(X) = X^{\varphi(n)} \Phi_n\left(\frac{1}{X}\right)$.

Le calcul de $X^{\varphi(n)} \Phi_n\left(\frac{1}{X}\right)$ donne :

$$X^{\varphi(n)} \Phi_n\left(\frac{1}{X}\right) = X^{\varphi(n)} \prod_{\omega \in \mathcal{P}_n} \underbrace{\left(\frac{1}{X} - \omega\right)}_{\varphi(n) \text{ termes}} = \prod_{\omega \in \mathcal{P}_n} X \left(\frac{1}{X} - \omega\right) = \prod_{\omega \in \mathcal{P}_n} (1 - \omega X) = \prod_{\omega \in \mathcal{P}_n} \omega \left(\frac{1}{\omega} - X\right) = \prod_{\omega \in \mathcal{P}_n} \omega \prod_{\bar{\omega} \in \mathcal{P}_n} (\bar{\omega} - X)$$

Selon le lemme 15 : $\prod_{\omega \in \mathcal{P}_n} \omega = 1$

$$X^{\varphi(n)} \Phi_n\left(\frac{1}{X}\right) = \prod_{\omega \in \mathcal{P}_n} (\bar{\omega} - X) = \underbrace{(-1)^{\varphi(n)}}_{=1 \text{ car } \varphi(n) \text{ pair}} \prod_{\omega \in \mathcal{P}_n} (X - \bar{\omega}) = \prod_{\bar{\omega} \in \mathcal{P}_n} (X - \bar{\omega}).$$

Et comme, selon le lemme 15 : $\omega \in \mathcal{P}_n \Leftrightarrow \bar{\omega} = \frac{1}{\omega} \in \mathcal{P}_n$, finalement $X^{\varphi(n)} \Phi_n\left(\frac{1}{X}\right) = \Phi_n(X)$.

Irréductibilité sur $\mathbb{Q}[X]$

Quelques précisions sur la notion d'irréductibilité

Dans un anneau intègre A , un élément $x \neq 0$ est dit irréductible s'il n'est pas inversible et si $x = yz$ ($y, z \in A$) \Rightarrow y ou z inversible. Par conséquent :

- ✓ Dans $\mathbb{Z}[X]$, $2X$ est réductible car le polynôme constant égal à 2 est non inversible ainsi que X .
- ✓ Dans $\mathbb{Q}[X]$, $2X$ est irréductible car le polynôme constant égal à 2 a pour inverse $\frac{1}{2}$.

De fait, dans $\mathbb{Z}[X]$, si un entier $1 < d$ divise tous les coefficients d'un polynôme non constant $P(X)$, ce dernier peut s'écrire : $P(X) = d\hat{P}(X)$ et est réductible. Pour les polynômes non constants, seuls ceux dont le PGCD des coefficients est égal à 1 peuvent être irréductibles.

17. Définition : polynôme primitif

Le contenu $\text{cont}(P)$ d'un polynôme $P \in \mathbb{Z}[X]$ non nul est le PGCD de ses coefficients.

P est dit primitif si et seulement si $\text{cont}(P) = 1$.

Exemple :

Un polynôme unitaire est primitif.

18. Proposition

Soit $P, Q \in \mathbb{Z}[X]$ non nuls :

1. Si P et Q sont primitifs, PQ aussi.
2. $\text{cont}(PQ) = \text{cont}(P) \times \text{cont}(Q)$

DEMONSTRATION :

1. Soit $P, Q \in \mathbb{Z}[X]$ primitifs. Supposons que PQ ne le soit pas. Il existe donc un nombre premier p divisant tous les coefficients de $P(X)Q(X) = \sum_{i=0}^n c_i X^i$. Considérons le morphisme d'anneau :

$$\mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X] \quad P(X) = \sum_{i=0}^n a_i X^i \mapsto \overline{P(X)} = \sum_{i=0}^n \overline{a_i} \overline{X^i}.$$

Comme les c_i sont tous des multiples de p $\overline{c_i} = 0$ dans $\mathbb{Z}/p\mathbb{Z}$ et par conséquent $\overline{PQ} = \overline{P}\overline{Q} = 0$. $\mathbb{Z}/p\mathbb{Z}[X]$ est un anneau intègre donc $\overline{P} = 0$ ou $\overline{Q} = 0$. Mais alors un des polynômes P ou Q a tous ses coefficients multiples de p . Contradiction.

2. Si $\text{cont}(P) = p$ et $\text{cont}(Q) = q$, on peut écrire : $P = pP_1$ et $Q = qQ_1$ où P_1, Q_1 sont primitifs. On alors : $\text{cont}(P) \times \text{cont}(Q) = pq$ et $\text{cont}(PQ) = \text{cont}(pqP_1Q_1) = pq \underbrace{\text{cont}(P_1Q_1)}_{=1} = pq$ puisque P_1Q_1 primitif.

19. Lemme

Soit $P \in \mathbb{Q}[X]$ non nul, alors il existe un entier $p > 0$ tel que le polynôme $pP \in \mathbb{Z}[X]$ et ait son contenu $\text{cont}(pP)$ premier avec p .

Si de plus, P est unitaire, pP est primitif.

DEMONSTRATION :

Soit $P(X) = \sum_{i=0}^n \frac{a_i}{b_i} X^i$, $a_i \in \mathbb{Z}, b_i \in \mathbb{N}^*$ après réduction des fractions $\frac{a_i}{b_i}$ à leur plus petit dénominateur commun p , on peut écrire : $P(X) = \frac{1}{p} \sum_{i=0}^n a'_i X^i$, $a'_i \in \mathbb{Z}$. Si il existait un facteur commun à p et aux a'_i , p ne serait pas le plus petit dénominateur commun. Donc p est premier avec le PGCD des a'_i égal à $\text{cont}(pP)$.

Si de plus P est unitaire, $1 = \frac{1}{p} a'_n$ et $a'_n = p$. Comme p est premier avec le PGCD des a'_i , ce dernier doit être égal à 1.

20. Proposition

Soit $P \in \mathbb{Z}[X]$ et $Q, R \in \mathbb{Q}[X]$. On suppose que deux de ces polynômes sont unitaires. Alors :

$$P = QR \Rightarrow Q \text{ et } R \in \mathbb{Z}[X]$$

DEMONSTRATION :

Remarquons au préalable que si deux de ces polynômes sont unitaires, le troisième l'est aussi.

Soit alors, selon le lemme 19 :

- ✓ q entier > 0 tel que $qQ \in \mathbb{Z}[X]$ et soit primitif.
- ✓ r entier > 0 tel que $rR \in \mathbb{Z}[X]$ et soit primitif.

On a alors $qrP = qQRrR$ primitif d'après la proposition 18. Mais ceci n'est possible que si $qr = 1$, ce qui implique $q = r = 1$ et alors : Q et $R \in \mathbb{Z}[X]$.

21. Proposition

Soit $P \in \mathbb{Z}[X]$ non constant, alors :

1. Si P n'est pas primitif, P est réductible sur $\mathbb{Z}[X]$
2. Si P est primitif :

$$P \text{ irréductible dans } \mathbb{Z}[X] \Leftrightarrow P \text{ irréductible dans } \mathbb{Q}[X]$$

DEMONSTRATION :

Le premier point a déjà été évoqué.

L'implication \Leftarrow est évidente.

Supposons P irréductible dans $\mathbb{Z}[X]$.

Si P est réductible dans $\mathbb{Q}[X]$, $P = QR$ $Q, R \in \mathbb{Q}[X]$. Soit alors, selon le lemme 19 :

- ✓ q entier > 0 tel que $Q_1 = qQ \in \mathbb{Z}[X]$ et q premier $\text{cont}(Q_1)$.
- ✓ r entier > 0 tel que $R_1 = rR \in \mathbb{Z}[X]$ et r premier $\text{cont}(R_1)$.

On alors : $P = \frac{1}{qr} Q_1 R_1$ où $P, Q_1, R_1 \in \mathbb{Z}[X]$. D'où $qr \text{cont}(P) = \text{cont}(Q_1 R_1)$. Or P est primitif et $\text{cont}(Q_1 R_1) = \text{cont}(Q_1) \text{cont}(R_1)$ d'après la proposition 18. Finalement :

$$qr = \text{cont}(Q_1) \text{cont}(R_1)$$

- ✓ Comme q premier avec $\text{cont}(Q_1)$, $q | \text{cont}(R_1)$.
- ✓ Comme r premier avec $\text{cont}(R_1)$, $r | \text{cont}(Q_1)$.

Il en résulte que $\frac{1}{q}R_1, \frac{1}{r}Q_1 \in \mathbb{Z}[X]$ et $P = \left(\frac{1}{r}Q_1\right)\left(\frac{1}{q}R_1\right)$ contredit l'irréductibilité de P dans $\mathbb{Z}[X]$.

Rappel sur le polynôme minimal d'un élément de \mathbb{C} sur \mathbb{Q}

Soit $\omega \in \mathbb{C}$. Comme il est racine du polynôme $X^n - 1$, il est algébrique sur \mathbb{Q} . L'ensemble des polynômes de $\mathbb{Q}[X]$ ayant ω comme racine est non vide et est un idéal I_ω de $\mathbb{Q}[X]$. Comme \mathbb{Q} est un corps, I_ω est principal et a pour générateur un unique polynôme unitaire $P_\omega(X)$ qui, par définition est le polynôme minimal de ω sur \mathbb{Q} .

$$I_\omega = P_\omega(X)\mathbb{Q}[X]$$

$P_\omega(X)$ est le polynôme unitaire de degré minimal ayant ω comme racine. Il vérifie les propriétés suivantes :

1. $P_\omega(X)$ est irréductible sur \mathbb{Q} .
2. Si un polynôme $T(X) \in \mathbb{Q}[X]$ a pour racine ω , il appartient à l'idéal I_ω et est un multiple de $P_\omega(X)$. En particulier pour $X^n - 1 = P_\omega(X)S(X)$ et $\Phi_n(X) = P_\omega(X)R(X)$.
3. ω est racine simple de $P_\omega(X)$.
4. Si α est une autre racine de $P_\omega(X)$, alors $P_\omega(X)$ est aussi le polynôme minimal de α .

Le théorème d'irréductibilité

Deux résultats préalables :

22. Proposition et définition : homomorphisme de Frobenius

Soit A un anneau de caractéristique p premier. L'application de $A \xrightarrow{f} A \quad x \mapsto x^p$ vérifie :

1. $f(x+y) = f(x) + f(y)$
2. $f(xy) = f(x)f(y)$

Et est donc un homomorphisme (dit de Frobenius) de l'anneau A dans lui-même.

DEMONSTRATION :

1. $f(x+y) = (x+y)^p = x^p + C_p^1 x^{p-1}y + \dots + C_p^{p-1} x y^{p-1} + y^p$
 $C_p^k = \frac{p(p-1)\dots(p-k+1)}{k!}$. Pour $1 \leq k \leq p-1$, les facteurs $\neq 1$ de $k!$ ne peuvent diviser p qui est premier. Il s'en suit que C_p^k est un multiple de p donc nul dans A .
2. Évident.

23. Lemme

Soit p premier, $\mathbb{Z}/p\mathbb{Z}[X]$ l'anneau des polynômes sur le corps $\mathbb{Z}/p\mathbb{Z}$ et $P(X) \in \mathbb{Z}/p\mathbb{Z}[X]$, alors : $(P(X))^p = P(X^p)$

DEMONSTRATION :

Soit $P(X) = \sum_{i=0}^n p_i X^i \in \mathbb{Z}/p\mathbb{Z}[X]$.

Comme $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p , $\mathbb{Z}/p\mathbb{Z}[X]$ aussi et le lemme précédent s'applique :

$$(P(X))^p = \sum_{i=0}^n p_i^p X^{pi} = \sum_{i=0}^n p_i^p (X^p)^i.$$

Comme $p_i \in \mathbb{Z}/p\mathbb{Z}$, le petit théorème de Fermat s'applique (cf 4) et $p_i^p = p_i$. Au final :

$$(P(X))^p = \sum_{i=0}^n p_i (X^p)^i = P(X^p)$$

24. Théorème

$\Phi_n(X)$ est irréductible sur $\mathbb{Q}[X]$, donc aussi sur $\mathbb{Z}[X]$.

DEMONSTRATION :

Soit $E = \{z \in \mathbb{C} / P_\omega(z) = 0\}$. Comme $\Phi_n(X)$ est multiple de $P_\omega(X)$, $E \subseteq \mathcal{P}_n$.

On va prouver que $\mathcal{P}_n \subseteq E$

$$X^n - 1 = P_\omega(X)S(X).$$

La proposition 20 indique que $P_\omega(X), S(X) \in \mathbb{Z}[X]$.

Si $\alpha \in E$, $\alpha^n = 1$. Soit p un nombre premier ne divisant pas n $(\alpha^p)^n = (\alpha^n)^p = 1$. $P_\omega(\alpha^p)S(\alpha^p) = 0$.

Supposons que $\alpha^p \notin E$ donc que $P_\omega(\alpha^p) \neq 0$. Donc $S(\alpha^p) = 0$ et α racine de $S(X^p)$. Alors $S(X^p)$ multiple de $P_\omega(X)$: $S(X^p) = P_\omega(X)T(X)$.

La proposition 20 indique que $T(X)$ aussi appartient à $\mathbb{Z}[X]$. On peut projeter sur $\mathbb{Z}/p\mathbb{Z}[X]$ ce qui donne en tenant compte du lemme 23 :

$$(\overline{S}(X))^p = \overline{S}(X^p) = \overline{P_\omega}(X)\overline{T}(X)$$

$\mathbb{Z}/p\mathbb{Z}[X]$ est anneau principal donc factoriel, tout facteur irréductible $\overline{R}(X)$ de $\overline{P_\omega}(X)$ divise $\overline{S}(X)$.

Mais on a aussi :

$$\overline{X^n - 1} = \overline{P_\omega}(X)\overline{S}(X) \text{ dans } \mathbb{Z}/p\mathbb{Z}[X]$$

Et alors $\overline{X^n - 1}$ posséderait un facteur irréductible au carré. Au quel cas $\overline{X^n - 1}$ et son polynôme dérivé $\overline{nX^{n-1}}$ aurait un facteur commun. Comme n et p premiers entre eux, n inversible dans $\mathbb{Z}/p\mathbb{Z}$, ce qui permet d'écrire :

$$\overline{X^n - 1} + n^{-1} \overline{X} \overline{nX^{n-1}} = 1$$

Or ceci est une égalité de Bezout qui dit que $\overline{X^n - 1}$ et $\overline{nX^{n-1}}$ sont premiers entre eux dans $\mathbb{Z}/p\mathbb{Z}[X]$.

En contradiction avec l'existence d'un facteur commun.

On a donc prouvé que si p est premier et ne divise pas n : $\alpha \in E \Rightarrow \alpha^p \in E$.

Soit maintenant $\beta \in \mathcal{P}_n$, β peut s'écrire $\beta = \omega^m$ où m premier avec n . m se décompose en produits de nombres premiers $m = \prod_{i=1}^k p_i$ où aucun des premiers p_i (non supposés distincts) ne divise n . En appliquant successivement le résultat précédent on aura :

$$\omega^{p_1} \in E, \omega^{p_1 p_2} = (\omega^{p_1})^{p_2} \in E, \dots, \omega^m = \omega^{p_1 p_2 \dots p_k} \in E$$

Donc $\beta \in E$. Mais alors les polynômes unitaires $\Phi_n(X)$ et $P_\omega(X)$ ont même racines et sont égaux. Comme par définition $P_\omega(X)$ est irréductible sur $\mathbb{Q}[X]$, $\Phi_n(X)$ aussi. Et comme $\Phi_n(X) \in \mathbb{Z}[X]$ et est unitaire, donc primitif, il est aussi irréductible sur $\mathbb{Z}[X]$.

Relations entre certains Φ_n

25. Proposition :

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

DEMONSTRATION :

Selon la proposition 14 :

$$\begin{aligned} \Phi_{pn}(X) &= \prod_{\substack{d|pn \\ d \not\equiv 0 \pmod{p}}} \left(X^{\frac{pn}{d}} - 1 \right)^{\mu(d)} = \prod_{d|n} \left(\left(X^p \right)^{\frac{n}{d}} - 1 \right)^{\mu(d)} \prod_{\substack{d|pn \\ d \not\equiv 0 \pmod{p}}} \left(X^{\frac{pn}{d}} - 1 \right)^{\mu(d)} \\ &= \Phi_n(X^p) \prod_{\substack{d|pn \\ d \not\equiv 0 \pmod{p}}} \left(X^{\frac{pn}{d}} - 1 \right)^{\mu(d)} \end{aligned}$$

1° cas : $p|n$

Alors $n = p^k q$ avec $1 \leq k$ et $p \wedge q = 1$, $pn = p^{k+1} q$. Les diviseurs d de pn sont de la forme : $d = p^s t$ avec $0 \leq s \leq k+1$ et $t|q$.

Si $0 \leq s \leq k$, d divise aussi $n = p^k q$. Les seuls diviseurs de pn ne divisant pas p sont donc de la forme $d = p^{k+1} t$. Comme $1 \leq k$, ils ont un facteur carré et $\mu(d) = 0$. Au final :

$$\prod_{\substack{d|pn \\ d \not\equiv 0 \pmod{p}}} \left(X^{\frac{pn}{d}} - 1 \right)^{\mu(d)} = \prod_{\substack{d|pn \\ d \not\equiv 0 \pmod{p}}} \left(X^{\frac{pn}{d}} - 1 \right)^0 = 1$$

2° cas : ~~$p|n$~~

Alors les diviseurs d de pn ne divisant pas p sont de la forme $d = pk$ où $k|n$. Alors :

$$\prod_{\substack{d|pn \\ d \not\equiv 0 \pmod{p}}} \left(X^{\frac{pn}{d}} - 1 \right)^{\mu(d)} = \prod_{k|n} \left(X^{\frac{pn}{pk}} - 1 \right)^{\mu(pk)}$$

Comme $p \wedge k = 1$, et μ multiplicative : $\mu(pk) = \mu(p)\mu(k)$. p étant premier, $\mu(p) = -1$. Au final :

$$\prod_{\substack{d|pn \\ d \not\equiv 0 \pmod{p}}} \left(X^{\frac{pn}{d}} - 1 \right)^{\mu(d)} = \prod_{k|n} \left(X^{\frac{pn}{pk}} - 1 \right)^{\mu(pk)} = \prod_{k|n} \left(X^{\frac{n}{k}} - 1 \right)^{-\mu(k)} = \frac{1}{\Phi_n(X)}$$

Application :

On avait établi précédemment : $\Phi_8(X) = X^4 + 1$. Alors :

1. $\Phi_{16}(X) = \Phi_{2 \times 8}(X) = \Phi_8(X^2) = X^8 + 1$ (cas 1)
2. $\Phi_{24}(X) = \Phi_{3 \times 8}(X) = \frac{\Phi_8(X^3)}{\Phi_8(X)} = \frac{X^{12} + 1}{X^4 + 1} = X^8 - X^4 + 1$ (cas 2)

Qu'en est-il sur un corps fini ?

Le résultat précédent s'avère alors faux.

Par exemple dans $\mathbb{Z}/17\mathbb{Z}$, où $1 = -16 \pmod{17}$, le polynôme cyclotomique $\Phi_8(X) = X^4 + 1$ peut s'écrire :

$$\Phi_8(X) = X^4 + 1 = X^4 - 16 = (X^2 - 4)(X^2 + 4) = (X - 2)(X + 2)(X^2 + 4)$$

Et est donc réductible. On peut même poursuivre sachant que $4 = -64 \pmod{17}$:

$$\Phi_8(X) = X^4 + 1 = (X - 2)(X + 2)(X^2 + 4) = (X - 2)(X + 2)(X^2 - 64) = (X - 2)(X + 2)(X - 8)(X + 8)$$

Le cas des corps finis fera l'objet d'une section à venir.

26. Corollaire

$$\text{Pour } 1 < n, \Phi_{2n}(X) = \begin{cases} \Phi_n(X^2) & \text{si } n \text{ est pair} \\ \Phi_n(-X) & \text{si } n \text{ est impair} \end{cases}$$

DEMONSTRATION :

La première formule est l'application immédiate du théorème précédent au cas $p = 2$. La deuxième

demande un peu plus de travail puisque ce théorème dans le cas n impair donne : $\Phi_{2n}(X) = \frac{\Phi_n(X^2)}{\Phi_n(X)}$.

$$\Phi_{2n}(X) = \frac{\Phi_n(X^2)}{\Phi_n(X)} = \frac{\prod_{d|n} \left(X^{\frac{2n}{d}} - 1 \right)^{\mu(d)}}{\prod_{d|n} \left(X^{\frac{n}{d}} - 1 \right)^{\mu(d)}} = \frac{\prod_{d|n} \left(X^{\frac{n}{d}} - 1 \right)^{\mu(d)} \left(X^{\frac{n}{d}} + 1 \right)^{\mu(d)}}{\prod_{d|n} \left(X^{\frac{n}{d}} - 1 \right)^{\mu(d)}} = \prod_{d|n} \left(X^{\frac{n}{d}} + 1 \right)^{\mu(d)}.$$

Or $\frac{n}{d}$ étant impair, on peut écrire :

$$\Phi_{2n}(X) = \prod_{d|n} \left(X^{\frac{n}{d}} + 1 \right)^{\mu(d)} = \prod_{d|n} (-1)^{\mu(d)} \left((-X)^{\frac{n}{d}} - 1 \right)^{\mu(d)} = (-1)^{\sum_{d|n} \mu(d)} \prod_{d|n} \left((-X)^{\frac{n}{d}} - 1 \right)^{\mu(d)}.$$

Or, pour $1 < n, \sum_{d|n} \mu(d) = 0$. Au final :

$$\Phi_{2n}(X) = \prod_{d|n} \left((-X)^{\frac{n}{d}} - 1 \right)^{\mu(d)} = \Phi_n(-X).$$

27. Proposition

Si les décompositions de n, m en facteurs premiers sont :

$$n = \prod_{i=1}^k p_i^{n_i} \quad \text{et} \quad m = \prod_{i=1}^k p_i^{m_i}$$

$$\text{Alors } \Phi_n(X) = \Phi_m \left(X^{\frac{n}{m}} \right)$$

DEMONSTRATION :

Si $m = n$, c'est évident.

Si $m \neq n$, cela signifie que n possède au moins un facteur carré. Alors les diviseurs de n ne divisant pas m sont ceux qui contiennent ce ou ces facteurs carrés.

Les diviseurs de m sont aussi des diviseurs de n . D'où :

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

Or si d divise n mais pas m , d a un facteur carré et $\mu(d) = 0$. D'où :

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

¹ On dit alors que m est le radical de n .

Application :

$$\Phi_{36}(X) = \Phi_{2 \times 3}\left(X^{\frac{36}{6}}\right) = \Phi_6(X^6) = X^{12} - X^6 + 1$$

Valeurs de $\Phi_n(1)$ et $\Phi_n(-1)$

28. Proposition

$$\Phi_n(1) = \begin{cases} 0 & \text{si } n = 1 \\ p & \text{si } n = p^r \text{ avec } p \text{ premier et } 1 \leq r \\ 1 & \text{sinon} \end{cases}$$

DEMONSTRATION :

1. Évident.
2. Si $r = 1$, n est premier, selon 11.5 : $\Phi_n(X) = 1 + X + \dots + X^{n-1}$.
Si $n = p^r$ avec p premier et $2 \leq r$, alors, $\Phi_n(X) = \Phi_{pp^{r-1}}(X)$ et selon la proposition 18
 $\Phi_n(X) = \Phi_{pp^{r-1}}(X) = \Phi_{p^{r-1}}(X^p)$. D'où $\Phi_n(1) = \Phi_{p^{r-1}}(1)$ et en itérant $\Phi_n(1) = \Phi_p(1) = p$.
3. Dans le cas restant, n peut s'écrire $n = p^r q$ où p est premier et ne divise pas q . On aura alors :

$$\Phi_n(1) = \Phi_{p^r q}(1) = \Phi_{p^{r-1} q}(1) = \dots = \Phi_{pq}(1) = \frac{\Phi_q(1)}{\Phi_q(1)} = 1$$

29. Proposition

$$\Phi_n(-1) = \begin{cases} -2 & \text{si } n = 1 \\ 0 & \text{si } n = 2 \\ 1 & \text{si } n \text{ est impair } > 1 \\ \Phi_{2^{k-1}m}(1) & \text{si } n = 2^k m \text{ où } m \text{ impair} \end{cases}$$

Dans le dernier cas, si $2^{k-1}m$ est une puissance d'un nombre premier p , ce qui advient soit si $k = 1$ et $m = p^r$, soit si $2 \leq k$ et $m = 1$, alors $\Phi_n(-1) = \Phi_{\underbrace{2^{k-1}m}_{=p^r}}(1) = p$. Sinon $\Phi_n(-1) = 1$.

DEMONSTRATION :

1. Évident.
2. Évident..
3. Si $1 < n$ est impair, le corollaire 19 donne : $\Phi_{2n}(X) = \Phi_n(-X)$. Donc $\Phi_n(-1) = \Phi_{2n}(1)$ et d'après la proposition 20 $\Phi_{2n}(1) = 1$.
4. Reste à traiter le cas n pair > 2 où n s'écrit : $n = 2^k m$ avec m impair. D'après le corollaire 20 $\Phi_{2^k m}(X) = \Phi_{2^{k-1}m}(-X)$. D'où $\Phi_n(-1) = \Phi_{2^{k-1}m}(1)$.

Avec Maple :

```
> for i from 20 to 32 do i, ifactor(i), cyclotomic(i,1), cyclotomic(i,-1); od;  
20, (2)2 (5), 1, 1  
21, (3) (7), 1, 1  
22, (2) (11), 1, 11  
23, (23), 23, 1  
24, (2)3 (3), 1, 1  
25, (5)2, 5, 1  
26, (2) (13), 1, 13  
27, (3)3, 3, 1  
28, (2)2 (7), 1, 1  
29, (29), 29, 1  
30, (2) (3) (5), 1, 1  
31, (31), 31, 1  
32, (2)5, 2, 2
```

Valeurs de coefficients

Les premiers exemples cités pour $\Phi_n(X)$ pouvaient suggérer que les coefficients appartenaient à $\{-1, 0, 1\}$. Mais l'exemple de $\Phi_{105}(X)$ calculé par Maple infirmait cette idée. Voici le moment d'examiner les choses de plus près...

30. Proposition

Soit k impair, n décomposé en facteurs premiers : $n = p_1 p_2 \cdots p_k$ avec $p_1 < p_2 < \cdots < p_k$ et $p_k < p_1 + p_2$. Alors le coefficient de X^{p_k} dans $\Phi_n(X)$ est $\pm 1 - k$.

Démonstration :

On notera : $F = \{p_1, p_2, \dots, p_k\}$.

Un diviseur de n est :

- ✓ Soit égal à 1
- ✓ Soit un produit de i ($1 \leq i \leq k$) éléments de F .

En notant, pour toute partie A non vide de F $\Pi(A)$ le produit de ses éléments, on définit :

$D_k^0 = \{1\}$ et pour $1 \leq i \leq k$, $D_k^i = \{\Pi(F_i) / F_i \subseteq F \text{ et } |F_i| = i\}$.

Autrement dit D_k^i est l'ensemble des diviseurs de n , produits de i facteurs parmi les k facteurs de n . On a :

- ✓ $D_k^1 = F = \{p_1, p_2, \dots, p_k\}$
- ✓ $D_k^k = \{p_1 p_2 \cdots p_k\} = \{n\}$
- ✓ $|D_k^i| = C_k^i$

L'ensemble des D_k^i , pour $0 \leq i \leq k$ est une partition de l'ensemble des diviseurs de n . D'où :

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu\left(\frac{n}{d}\right)} = \prod_{d \in D_k^0} (X^d - 1)^{\mu\left(\frac{n}{d}\right)} \times \prod_{d \in D_k^1} (X^d - 1)^{\mu\left(\frac{n}{d}\right)} \times \cdots \times \prod_{d \in D_k^k} (X^d - 1)^{\mu\left(\frac{n}{d}\right)}$$

On projette sur $\mathbb{C}[X] / (X^{p_k+1})$.

Alors tous les X^d pour $d \in D_k^2 \cup D_k^3 \cup \cdots \cup D_k^k$ sont nuls puisqu'alors $d \geq p_1 p_2 > p_1 + p_2 > p^k$

$$\overline{\Phi_n(X)} = (X - 1)^{\mu(n)} \times \prod_{i \in 1 \cdots k} (X^{p_i} - 1)^{\mu\left(\frac{n}{p_i}\right)} \times \prod_{d \in D_k^1} (-1)^{\mu\left(\frac{n}{d}\right)} \times \cdots \times \prod_{d \in D_k^k} (-1)^{\mu\left(\frac{n}{d}\right)}.$$

Comme k impair, $\mu(n) = -1$, $\mu\left(\frac{n}{p_1 \cdots p_k}\right) = 1$. Par ailleurs, pour $d \in D_k^i$ avec $i \in 2 \cdots k$ $\mu\left(\frac{n}{d}\right) = \pm 1$

donc $\prod_{d \in D_k^i} (-1)^{\mu\left(\frac{n}{d}\right)} = -1$ et comme $2 \cdots k$ a un nombre pair d'éléments leur produit vaut 1. Donc :

$$\overline{\Phi_n(X)} = (X - 1)^{-1} \times \prod_{i \in 1 \cdots k} (X^{p_i} - 1)$$

Comme : $\frac{X^{p_k} - 1}{X - 1} = X^{p_k-1} + \cdots + X + 1$,

$$\overline{\Phi_n(X)} = (X^{p_1} - 1) \cdots (X^{p_{k-1}} - 1) (X^{p_k-1} + \cdots + X + 1).$$

Lorsque l'on développe le produit des $k-1$ premiers facteurs, tous les termes issus de 2 ou plus des X^{p_i} auront un exposant strictement supérieur à p_k et seront donc nuls dans $\mathbb{C}[X] / (X^{p_k+1})$.

$$\overline{\Phi_n(X)} = (1 - X^{p_1} - X^{p_2} \dots - X^{p_{k-1}}) (X^{p_k-1} + \dots + X + 1).$$

L'ensemble $0 \dots p_k - 1$ des exposants du terme de droite contient les entiers :

$$p_k - p_1, p_k - p_2, \dots, p_k - p_{k-1}$$

Il s'en suit que le terme de degré p_k dans le produit va être obtenu par les choix :

Choix dans le 1° facteur	Choix dans le 2° facteur
$-X^{p_1}$	$X^{p_k-p_1}$
\vdots	\vdots
$-X^{p_i}$	$X^{p_k-p_i}$
\vdots	\vdots
$-X^{p_{k-1}}$	$X^{p_k-p_{k-1}}$

Son coefficient va donc être : $1 - k$.

Exemples :

En dehors de $105 = 5 \times 7 \times 11$, déjà vu, on peut citer :

$$\checkmark \quad 715 = 5 \times 11 \times 13 \quad (\text{la proposition n'exige pas que les } p_i \text{ soient des premiers consécutifs}).$$

ou encore avec $k = 5$

$$\checkmark \quad 1\,065\,347 = 11 \times 13 \times 17 \times 19 \times 23.$$

En fait les listes (p_1, p_2, \dots, p_k) de premiers vérifiant les conditions requises sont beaucoup plus abondantes que ce que l'on pourrait penser. Par exemple, pour $k = 13$, les commandes suivantes de Maple :

```
> P100 := [seq(ithprime(i), i=2..100)] (liste des 100 premiers premiers)
> k:=13; j:=1; for i from 3 to nops(P100)-k+1 do if P100[i]+P100[i+1]>P100[i+k-1] then print(j,P100[i..i+k-1]); j:=j+1; fi; od;
```

en déterminent 73 (en se limitant aux premiers consécutifs) depuis :

$$1, [53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107]$$

jusqu'à :

$$73, [457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541]$$

Se pose la question de savoir si pour, pour tout k impair, on peut trouver $n = p_1 p_2 \dots p_k$ avec $p_1 < p_2 < \dots < p_k$ et $p_k < p_1 + p_2$? En cas de réponse positive, cela signifierait que des coefficients de $\Phi_n(X)$ peuvent être arbitrairement grand.

31. Proposition

Pour tout entier k impair, il existe une liste de (p_1, p_2, \dots, p_k) de nombres premiers vérifiant :

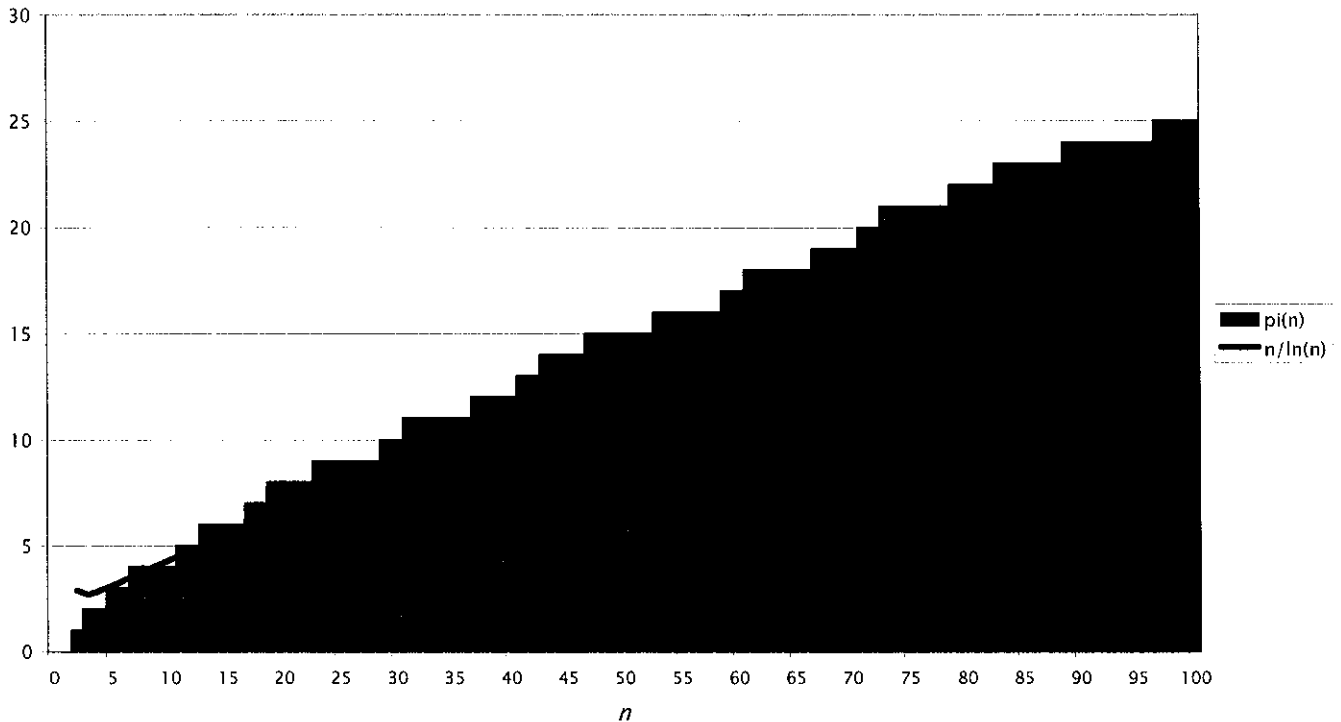
1. $p_1 < p_2 < \dots < p_k$
2. $p_k < p_1 + p_2$.

DEMONSTRATION :

S'il existe k tel qu'aucune liste (p_1, p_2, \dots, p_k) ne vérifie les conditions, alors $2p_1 < p_k$. En notant m , le plus grand entier tel que $2^m < p_1$, il s'en suivrait que chaque intervalle $[2^{m-1}, 2^m[$ contiendrait strictement moins de k nombre premiers. Le nombre de premiers appartenant à $[1, 2^m[= \bigcup_{j=1}^m [2^{j-1}, 2^j[$

serait alors strictement inférieur à km . Le nombre $\pi(2^m)$ de premiers $\leq 2^m$ serait alors strictement inférieur à km . Or la fonction π de comptage des nombres premiers $\leq x$ vérifie la minoration : $\frac{x}{\ln(x)} < \pi(x)$ dès que $11 \leq x$. D'où : $\frac{2^m}{m \ln(2)} < \pi(2^m)$. Mais pour m suffisamment grand $km < \frac{2^m}{m \ln(2)}$. Contradiction.

Comparaison $\pi(n)$ et $n/\ln(n)$ et $Li(n)$



Dans cet ordre d'idée, il existe un résultat du à EMMA LEHMER :

Théorème

Soit $n = pqr$ où p , $q = ap + 2$ et $r = \frac{bpq - 1}{2}$ sont premier, alors le coefficient de $X^{\frac{(p-3)(qr+1)}{2}}$ dans $\Phi_n(X)$ est égal à $\frac{p-1}{2}$.

On en trouvera une démonstration (assez compliquée) dans [3]. Le théorème de Dirichlet justifie l'existence de q et r premiers.

Exemple :

$p = 7$, $q = 3 \times 7 + 2 = 23$, $r = \frac{3 \times 7 \times 23 - 1}{2} = 241$ D'où :

$n = pqr = 7 \times 23 \times 241 = 38801$ $\frac{(p-3)(qr+1)}{2} = \frac{4 \times (23 \times 241 + 1)}{2} = 11088$. Le coefficient de X^{11088} dans

$\Phi_{38801}(X)$ doit être égal à $\frac{p-1}{2} = 3$. Ce que Maple arrive à vérifier en ≈ 28 secondes.

```
> t:=time():coeff(cyclotomic(7*23*241,X),X,11088);duree_calcul:=time()-t;
3
duree_calcul := 27.971
```

Notations

$ E $	Nombre d'éléments d'un ensemble fini E .
$m \cdots n$	ensemble des entiers i $m \leq i \leq n$
$m \wedge n$	PGCD des entiers m et n .
$m n$	L'entier m divise l'entier n .
φ	Fonction indicatrice d'Euler : $\varphi(n) = \left \left\{ k \text{ entier} / 1 \leq k \leq n \text{ et } k \wedge n = 1 \right\} \right $
μ	Fonction de Mobius
\mathcal{P}_n	l'ensemble des $\varphi(n)$ racines $n^{\text{ème}}$ primitives de l'unité dans \mathbb{C} .
$A[X]$	Anneau des polynômes sur l'anneau A .
$\Phi_n(X)$	Le n -ième polynôme cyclotomique : $\Phi_n(X) = \prod_{\omega \in \mathcal{P}_n} (X - \omega) = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} (X - \omega^k)$
$\mathbb{Z}/n\mathbb{Z}$	Anneau (corps si n premier) des entiers modulo n .
A/I	Quotient de l'anneau A par l'idéal I .
$aA, (a)$	Idéal principal de l'anneau A engendré par a .
$\text{cont}(P)$	Le contenu d'un polynôme $P \in \mathbb{Z}[X]$ non nul défini comme le PGCD des coefficients.