Polinômios Ciclotômicos e o Teorema dos Primos de Dirichlet

Antonio Caminha

15 de fevereiro de 2003

Resumo

Neste artigo definimos e provamos as principais propriedades dos polinômios ciclotômicos, objetivando demonstrar um caso particular do famoso teorema de Dirichlet sobre primos em progressões aritméticas.

1 Preliminares.

No que segue, denotaremos por $\mathbb{Z}$ o conjunto dos inteiros e por $\mathbb{N}$ o conjunto dos inteiros positivos. Dado um primo p, $\mathbb{Z}_p$ é o anel das classes de congruência módulo p, i.e.,

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$$

munido com as operações $+$ e $\cdot$ dadas por

$$\overline{x} + \overline{y} = \overline{x+y} \quad \text{e} \quad \overline{x} \cdot \overline{y} = \overline{xy},$$

onde $x, y \in \mathbb{Z}$ e as operações sob as barras nos segundos membros das igualdades acima são a adição e a multiplicação usuais de $\mathbb{Z}$. É imediato verificar que tais operações sobre $\mathbb{Z}_p$ gozam de propriedades análogas às operações correspondentes sobre $\mathbb{Z}$. Ademais, dado $\overline{x} \neq \overline{0}$ em $\mathbb{Z}_p$, existe um único $\overline{y} \in \mathbb{Z}_p$ tal que $\overline{x} \cdot \overline{y} = \overline{1}$, de modo que $\mathbb{Z}_p$ é um *corpo*[1]. Doravante, sempre que não houver perigo de confusão, denotaremos $\overline{x} \in \mathbb{Z}_p$ simplesmente por x.

A letra $\mathbb{K}$ representará sempre um dos corpos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ou $\mathbb{Z}_p$, p primo, ao passo que $\mathbb{K}[X]$ denotará o anel dos polinômios sobre (i.e., com coeficientes em) $\mathbb{K}$. Dado $f \in \mathbb{K}[X]$, digamos

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + a_{n-2} X^{n-2} + \cdots + a_2 X^2 + a_1 X + a_0,$$

[1] Veja também [3] e o capítulo 1 de [2].

sua *derivada* f' é o polinômio sobre $\mathbb{K}$ dado por

$$f'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + 2a_2X + a_1.$$

Dados $f, g \in \mathbb{K}[X]$, é imediato verificar que

$$(f+g)'(X) = f'(X) + g'(X) \text{ e } (fg)'(X) = f'(X)g(X) + f(X)g'(X).$$

Por fim, um polinômio sobre $\mathbb{K}$ é dito *mônico* quando seu coeficiente líder for $1 \in \mathbb{K}$.

2 Fatoração de polinômios.

Definição 1 (Polinômio irredutível). *Seja $f \in \mathbb{K}[X]$ um polinômio não constante. Dizemos que f é irredutível sobre $\mathbb{K}$ (ou simplesmente irredutível, quando $\mathbb{K}$ estiver subentendido) se f não puder ser escrito como um produto de dois polinômios sobre $\mathbb{K}$, não constantes. Caso contrário, f é redutível sobre $\mathbb{K}$.*

Note que um polinômio não constante em $\mathbb{K}[X]$, de grau 1, é automaticamente irredutível. Os polinômios em $\mathbb{K}[X]$ irredutíveis desempenham, em $\mathbb{K}[X]$, papel análogo ao desempenhado pelos números primos em $\mathbb{Z}$. O resultado a seguir, análogo do teorema fundamental da aritmética em $\mathbb{Z}$, dá mais clareza a tal observação. O leitor interessado pode encontrar uma demonstração do mesmo, para $\mathbb{K}$ corpo qualquer, em [2].

Proposição 2 (Fatoração única). *Todo polinômio sobre $\mathbb{K}$, mônico e não constante, pode ser expresso como produto de polinômios sobre $\mathbb{K}$, mônicos, não constantes e irredutíveis. Ademais, tal representação é única a menos de uma reordenação dos fatores.*

Corolário 3. *Seja $f \in \mathbb{K}[X]$ irredutível e $g, h \in \mathbb{K}[X] \setminus \{0\}$ tais que $f \mid gh$. Então $f \mid g$ ou $f \mid h$.*

Prova. Podemos supor, sem perda de generalidade, f mônico. Se g ou h for constante, nada há a fazer. Senão, seja $l \in \mathbb{K}[X]$ tal que $fl = gh$ $(*)$. Pela proposição 2, podemos escrever cada um dos polinômios g, h, l como um produto de polinômios irredutíveis sobre $\mathbb{K}$. Segue então de $(*)$ e da parte unicidade na proposição 2 que f é um dos fatores de g ou um dos fatores de h, i.e., que $f \mid g$ ou $f \mid h$. □

Proposição 4 (Fatores múltiplos). *Seja $f \in \mathbb{K}[X]$ um polinômio não constante. Se f tiver um fator múltiplo g então $g \mid f'$ em $\mathbb{K}[X]$. Reciprocamente, se $g \in \mathbb{K}[X]$ irredutível for tal que $g \mid f$ e $g \mid f'$, com $p \nmid \partial g$ caso $\mathbb{K} = \mathbb{Z}_p$, p primo, então $g^2 \mid f$.*

PROVA. Seja $h \in \mathbb{K}[X]$ tal que $f(X) = g(X)^2 h(X)$. Então

$$f'(X) = g(X)[2g'(X)h(X) + g(X)h'(X)].$$

donde $g \mid f'$. Reciprocamente, seja $g \in \mathbb{K}[X]$ irredutível tal que $g \mid f$, $g \mid f'$. Então existem $u, v \in \mathbb{K}[X]$ tais que $f = gu$, $f' = gv$. As hipóteses sobre g garantem que $g' \neq 0$. Por outro lado, a igualdade $f = gu$ nos dá $f' = g'u + gu'$, ou ainda $g(v - u') = g'v$. Logo, g divide $g'u$ e segue do corolário anterior que $g \mid u$. Se $t \in \mathbb{K}[X]$ for tal que $u = gt$, temos então $f = g^2 t$. □

Em princípio, poderia ocorrer de um polinômio $f \in \mathbb{Z}[X]$ não poder ser escrito como produto de dois polinômios não constantes sobre $\mathbb{Z}$ mas ser redutível sobre $\mathbb{Q}$. Mostremos que tal não pode acontecer.

Lema 5 (Gauss).

(a) *Seja $f \in \mathbb{Z}[X]$. Se f não puder ser escrito como produto de dois polinômios não constantes de coeficientes inteiros então f é irredutível sobre $\mathbb{Q}$.*

(b) *Para cada $f \in \mathbb{Z}[X]$, seja $c(f)$ o mdc dos coeficientes não nulos de f. Dados $f, g \in \mathbb{Z}[X]$, temos $c(fg) = c(f)c(g)$.*

PROVA.
(a) Sejam $g, h \in \mathbb{Q}[X]$ polinômios não constantes tais que $f = gh$. Então existe um menor $m \in \mathbb{N}$ tal que $mf(X) = g_1(X)h_1(X)$, com $g_1, h_1 \in \mathbb{Z}[X]$ múltiplos inteiros de g, h, respectivamente. Sejam

$$g_1(X) = a_r X^r + \cdots + a_1 X + a_0, \quad h_1(X) = b_s X^s + \cdots + b_1 X + b_0.$$

Se $m > 1$, tome um primo p que divide m. Provemos que $p \mid a_i$ para todo i ou $p \mid b_j$ para todo j. Supondo o contrário, existem índices i, j tais que $p \nmid a_i$ e $p \nmid b_j$, mínimos com tal propriedade. Como $p \mid m$, segue que p divide o coeficiente de X^{i+j} em $mf(X) = g_1(X)h_1(X)$, quer dizer, p divide

$$\cdots + a_{i+2}b_{j-2} + a_{i+1}b_{j-1} + a_i b_j + a_{i-1}b_{j+1} + a_{i-2}b_{j+2} + \cdots \quad (*)$$

Mas a minimalidade de i e j garante que p divide $a_0, a_1, \ldots, a_{i-1}$ e $b_0, b_1, \ldots, b_{j-1}$. Portanto, segue de $(*)$ que $p \mid a_i b_j$, o que é um absurdo.

Suponhamos pois, sem perda de generalidade que $p \mid a_i$ para todo i. Então existe um polinômio $g_2 \in \mathbb{Z}[X]$ tal que $g_1(X) = pg_2(X)$. Se $m = pm_1$, com $m_1 \in \mathbb{N}$, obtemos $m_1 f(X) = g_2(X)h_1(X)$, o que contraria a minimalidade de m. Logo, $m = 1$ e f pode ser escrito como um produto de dois polinômios não constantes e de coeficientes inteiros.

(b) Exercício. □

Dado $f \in \mathbb{Z}[X]$ não constante, dizemos que f é *primitivo* quando $c(f) = 1$. Em $\mathbb{Q}[X]$, seja $f = f_1 \cdots f_k$, onde $f_1, \ldots, f_k$ são irredutíveis em $\mathbb{Q}[X]$. Pelo item (a) do lema de Gauss podemos supor que $f_1, \ldots, f_k \in \mathbb{Z}[X]$. Pelo item (b), temos

$$1 = c(f) = c(f_1) \cdots c(f_k),$$

de modo que $c(f_i) = 1$ para todo i, ou seja, cada f_i é primitivo. Obtivemos então, essencialmente a seguinte

Proposição 6. *Todo polinômio de coeficientes inteiros, primitivo e não constante, pode ser expresso, de modo único a menos de reordenação dos fatores, como um produto de polinômios de coeficientes inteiros, primitivos e não constantes, irredutíveis sobre* $\mathbb{Q}$.

Dado um primo p, definimos a aplicação de projeção

$$\pi_p : \mathbb{Z}[X] \longrightarrow \mathbb{Z}_p[X]$$

pondo, para $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$,

$$\overline{f}(X) = \pi_p(f(X)) = \overline{a}_n X^n + \cdots + \overline{a}_1 X + \overline{a}_0.$$

Observe que se $p \nmid a_n$ então $\partial \overline{f} = \partial f$.

Proposição 7. *Seja* $f \in \mathbb{Z}[X]$ *e* p *um número primo então* $\overline{f}(X^p) = \overline{f}(X)^p$.

Prova. Seja $f(X) = a_n X^n + \cdots + a_1 X + a_0$. Queremos mostrar que

$$\overline{a_n} X^{np} + \overline{a_{n-1}} X^{(n-1)p} \cdots + \overline{a_1} X^p + \overline{a_0} = (\overline{a_n} X^n + \overline{a_{n-1}} X^{n-1} \cdots + \overline{a_1} X + \overline{a_0})^p. \quad (*)$$

Façamos indução sobre $n \geq 1$. Para $n = 1$ temos de mostrar que

$$\overline{a_1} X^p + \overline{a_0} = (\overline{a_1} X + \overline{a_0})^p. \quad (**)$$

Se $p \mid a_1$, $(**)$ é o pequeno teorema de Fermat. Senão, $(**)$ segue imediatamente a partir do desenvolvimento do binômio e do fato de que $p \mid \binom{p}{k}$ para todo inteiro $1 \leq k < p$.

Suponha agora a validez de $(*)$ para $n < m$ e todo polinômio de coeficientes inteiros e grau m. Seja $f \in \mathbb{Z}[X]$ de grau m, digamos $f(X) = a_m X^m + g(X)$, com $\partial g < m$. Por hipótese de indução, temos $\overline{g}(X^p) = \overline{g}(X)^p$. O mesmo argumento acima, juntamente com o pequeno teorema de Fermat, nos dão

$$\begin{aligned} \overline{f}(X)^p &= (\overline{a_m} X^m + \overline{g}(X))^p = (\overline{a_m})^p X^{mp} + \overline{g}(X)^p \\ &= \overline{a_m} X^{mp} + \overline{g}(X^p) = \overline{f}(X^p). \end{aligned}$$

□

Corolário 8 (Critério de Eisenstein). *Seja $f(X) = a_nX^n + \cdots + a_1X + a_0$ um polinômio não constante de coeficientes inteiros e p um primo tal que:*

(a) $p \mid a_0, a_1, \ldots, a_{n-1}$.

(b) $p^2 \nmid a_0$ *e* $p \nmid a_n$.

Então f é irredutível sobre $\mathbb{Q}$.

Prova. Suponha $f = gh$, com g e h polinômios não constantes de coeficientes inteiros. Como $p \nmid a_n$, p não divide os coeficientes líderes b de g e c de h. Projetando f em $\mathbb{Z}_p[X]$, obtemos

$$\overline{a_n}X^n = \overline{g}(X)\overline{h}(X).$$

A proposição 2 garante que $\overline{g}(X) = \overline{b}X^k$ e $\overline{h}(X) = \overline{c}X^l$, onde $k = \partial g \geq 1$ e $l = \partial h \geq 1$. Então existem $u, v \in \mathbb{Z}[X]$ tais que

$$g(X) = bX^k + pu(X) \quad \text{e} \quad h(X) = cX^l + pv(X).$$

Por fim,

$$f(X) = g(X)h(X) = bcX^n + p(cX^l u(X) + bX^k v(X)) + p^2 u(X)v(X),$$

de modo que $a_0 = f(0) = g(0)h(0) = p^2u(0)v(0)$, um múltiplo de p^2, o que é um absurdo. □

Lema 9. *Seja f um polinômio não constante de coeficientes racionais, a um racional dado e $g(X) = f(X + a)$. Então f é irredutível sobre $\mathbb{Q}$ se e só se g o for.*

Prova. Exercício. □

Corolário 10. *Seja p um número primo e $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Então f é irredutível sobre $\mathbb{Q}$.*

Prova. Basta mostrarmos que $g(X) = f(X + 1)$ é irredutível sobre $\mathbb{Q}$. Mas

$$g(X) = (X + 1)^{p-1} + (X + 1)^{p-2} + \cdots + (X + 1) + 1$$

e é fácil vermos que, para $1 \leq k \leq p - 2$, o coeficiente a_k de X^k em g é

$$a_k = \binom{p-1}{k} + \binom{p-2}{k} + \binom{p-3}{k} + \cdots + \binom{k}{k} = \binom{p}{k+1},$$

que sabemos ser múltiplo de p. Como

$$g(X) = X^{p-1} + a_{p-2}X^{p-2} + \cdots + a_1X + p,$$

segue do critério de Eisenstein aplicado ao primo p que g é irredutível sobre $\mathbb{Q}$. □

No que segue, dados $f \in \mathbb{C}[X]$ e $\alpha \in \mathbb{C}$, dizemos que f anula α se $f(\alpha) = 0$. Um número complexo α é dito *algébrico sobre* $\mathbb{Q}$ se existir um polinômio $f \in \mathbb{Q}[X] \setminus \{0\}$ que anula α. Nesse caso, o conjunto

$$\mathcal{A}_\alpha = \{f \in \mathbb{Q}[X] \setminus \{0\};\, f(\alpha) = 0\}$$

é, por definição, não-vazio; portanto, é também não-vazio o conjunto

$$\partial_\alpha = \{\partial f;\, f \in \mathcal{A}_\alpha\},$$

de modo que existe $p_\alpha \in \mathcal{A}_\alpha$ mônico e de grau mínimo.

Definição 11 (Polinômio minimal). *Dado $\alpha \in \mathbb{C}$ algébrico sobre $\mathbb{Q}$, o polinômio $p_\alpha \in \mathbb{Q}[X] \setminus \{0\}$, mônico, de grau mínimo e que anula α é denominado o polinômio minimal de α.*

Proposição 12 (Propriedades do polinômio minimal). *Seja α algébrico sobre $\mathbb{Q}$ e p_α seu polinômio minimal. Então:*

(a) *p_α é irredutível sobre $\mathbb{Q}$.*

(b) *p_α divide, em $\mathbb{Q}[X]$, todo polinômio de coeficientes racionais que anula α.*

Prova.
(a) Se $p_\alpha = fg$, com f e g não constantes e de coeficientes racionais, então f e g teriam graus menores que o grau de p_α e ao menos um deles anularia α, contradizendo a minimalidade do grau de p_α. Logo, p_α é irredutível.

(b) Seja $f \in \mathbb{Q}[X]\setminus\{0\}$ um polinômio que anula α. Pelo algoritmo da divisão existem polinômios $q, r \in \mathbb{Q}[X]$ tais que

$$f(X) = p_\alpha(X)q(X) + r(X),$$

com $r(X) = 0$ ou $0 \leq \partial r < \partial p_\alpha$. Se $r \neq 0$ então

$$r(\alpha) = f(\alpha) - p_\alpha(\alpha)q(\alpha) = 0,$$

com $\partial r < \partial p_\alpha$, o que é um absurdo. Logo, $r = 0$ e daí $p_\alpha \mid f$. □

Corolário 13. *Se α é algébrico sobre $\mathbb{Q}$ e $f \in \mathbb{Q}[X]$ é um polinômio mônico irredutível que anula α então $f = p_\alpha$.*

Prova. Pela proposição anterior, p_α divide f em $\mathbb{Q}[X]$. Mas como f é irredutível, existe um racional não nulo r tal que $f = rp_\alpha$. Por fim, desde que f e p_α são mônicos temos $r = 1$. □

Corolário 14. *Se $f \in \mathbb{Q}[X]$ é irredutível então f não possui raízes múltiplas.*

PROVA. Podemos supor, sem perda de generalidade, que f é mônico. Se algum $z \in \mathbb{C}$ fosse raiz múltipla de f, segue da proposição 4 que z também seria raiz da derivada f' de f. Mas f mônico e irredutível assegura, pelo corolário anterior, que $f = p_z$. Então, o item (b) da proposição 12 garante que $f \mid f'$ em $\mathbb{Q}[X]$, o que é um absurdo. □

3 Polinômios ciclotômicos e o teorema de Dirichlet.

Dizemos que um número complexo z é uma *raiz $n-$ésima da unidade* quando $z^n = 1$, ou seja, quando $z \in \mathbb{C}$ for uma das raízes do polinômio $X^n - 1 \in \mathbb{C}[X]$. Segue então das fórmulas de de Moivre que as raízes $n-$ésimas da unidade são os números complexos da forma

$$\cos \frac{2k\pi}{n}; \quad 0 \leq k \leq n-1.$$

Uma raiz $n-$ésima da unidade ω é dita *primitiva* quando os números ω^k, $0 \leq k \leq n-1$, forem todos distintos. Em particular, o número $\cos \frac{2\pi}{n}$ é uma raiz primitiva $n-$ésima da unidade e não é difícil verificar que $\cos \frac{2k\pi}{n}$ é uma raiz primitiva $n-$ésima da unidade se e só se $\text{mdc}\,(k,n) = 1$.

Definição 15 (Polinômios ciclotômico). *Para cada $n \in \mathbb{N}$, o polinômio minimal Φ_n da raiz primitiva $n-$ésima da unidade $\omega_n = \cos 2\pi/n$ é denominado o $n-$ésimo polinômio ciclotômico.*

Teorema 16 (Polinômios ciclotômicos). *Os itens a seguir se verificam:*

(a) $\Phi_1(X) = X - 1$.

(b) *Se p é primo então* $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.

(c) *Se $r, s \in \mathbb{N}$ são distintos então Φ_r e Φ_s não têm fatores comuns não constantes.*

(d) *Se $n \in \mathbb{N}$ e $0 < d \mid n$ então $\Phi_d \mid (X^n - 1)$ em $\mathbb{Q}[X]$. Em particular, $\Phi_n(X) \in \mathbb{Z}[X]$ para todo $n \in \mathbb{N}$.*

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

(f) $\Phi_n(X) = \prod_{\substack{1 \leq k < n \\ \text{mdc}(k,n)=1}} (X - \omega^k)$.

(g) $\partial\Phi_n = \varphi(n)$, *onde $\varphi : \mathbb{N} \to \mathbb{N}$ é a função de Euler*[2].

[2]Para a definição e algumas propriedades importantes da função de Euler, veja [3] ou [5].

PROVA.
(a) Óbvio.

(b) Já mostramos que o polinômio $X^{p-1} + X^{p-2} + \cdots + X + 1$ é irredutível. Como

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

e ω_p é raiz de $X^p - 1$ mas não de $X - 1$, segue que ω_p é raiz de $X^{p-1} + X^{p-2} + \cdots + X + 1$. Portanto, segue do corolário 13 que $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.

(c) Sejam r e s naturais distintos e suponha que Φ_r e Φ_s tivessem um fator comum não constante. Então eles seriam idênticos, como polinômios minimais de uma qualquer de suas raízes comuns.

(d) Sejam $n \in \mathbb{N}$ e $0 < d \mid n$. Como toda raiz $d-$ésima da unidade é também raiz $n-$ésima da unidade, segue que toda raiz de Φ_d é raiz de $X^n - 1$. Portanto, Φ_d divide $X^n - 1$ em $\mathbb{Q}[X]$, por ser Φ_d o polinômio minimal de uma qualquer de suas raízes. O resto segue do lema de Gauss.

(e), (f) e (g). Seja $\omega = \text{cis}\,\frac{2\pi}{n}$. Mostremos primeiro que

$$\Phi_n(X) = \prod_{\substack{1 \leq k < n \\ \text{mdc}(k,n)=1}} (X - \omega^k).$$

Se ζ é uma raiz $n-$ésima da unidade então $p_\zeta(X)$ divide $X^n - 1$ em $\mathbb{Q}[X]$. Portanto, segue da proposição 6 que $p_\zeta \in \mathbb{Z}[X]$. Tome $1 \leq k < n$ primo com n, p um primo que divide k e faça $\zeta = \omega^p$. Por contradição, suponha que $p_\zeta \neq p_\omega = \Phi_n$. Como ambos estes polinômios são irredutíveis e dividem $X^n - 1$, existe um polinômio $u \in \mathbb{Z}[X]$ tal que

$$p_\zeta(X)p_\omega(X)u(X) = X^n - 1. \quad (*)$$

Se $g(X) = p_\zeta(X^p)$, temos

$$g(w) = p_\zeta(\omega^p) = p_\zeta(\zeta) = 0.$$

Daí, p_ω divide g em $\mathbb{Z}[X]$. Seja $v \in \mathbb{Z}[X]$ tal que $p_\omega v = g$. Em $\mathbb{Z}_p[X]$, temos

$$\overline{p}_\omega(X)\overline{v}(X) = \overline{g}(X) = \overline{p}_\zeta(X^p) = \left(\overline{p}_\zeta(X)\right)^p.$$

Então existe $\overline{h} \in \mathbb{Z}_p[X]$ mônico, irredutível e tal que $\overline{h}$ divide p_ω e $\overline{p}_\zeta$ em $\mathbb{Z}_p[X]$. Assim, $(*)$ garante que $\overline{h}^2$ divide $X^n - \overline{1}$ em $\mathbb{Z}_p[X]$. Pela proposição 4, segue que $\overline{h}$ divide $(X^n - \overline{1})' = \overline{n}X^{n-1}$ em $\mathbb{Z}_p[X]$. Como $p \nmid n$, segue então da fatoração única em $\mathbb{Z}_p[X]$ que $\overline{h}(X) = X^l$ para algum $1 \leq l \leq n-1$, o que contraria o fato de $\overline{h}$ dividir $X^n - \overline{1}$. Concluímos então que $p_\zeta = p_\omega$, ou ainda que $p_{\omega^p} = p_\omega$.

Iterando o raciocínio acima, concluímos que $p_\omega = p_{\omega^p} = p_{\omega^{p^2}} = \cdots = p_{\omega^k}$. Em particular, ω^k é raiz de $p_\omega = \Phi_n$, de modo que Φ_n é divisível pelo polinômio

$$\prod_{\substack{1\leq k<n \\ \text{mdc}(k,n)=1}} (X - \omega^k).$$

Mas como o grau de tal polinômio é $\varphi(n)$, obtemos que $\partial\Phi_n \geq \varphi(n)$. Por outro lado, segue dos itens (c) e (d) que

$$\Phi(X) = \prod_{0<d|n} \Phi_d(X)$$

divide $X^n - 1$. Mas então

$$n \geq \partial\Phi = \sum_{0<d|n} \partial\Phi_d \geq \sum_{0<d|n} \varphi(d) = n,$$

onde a última igualdade se deve a uma conhecida propriedade da função φ de Euler[3]. Então $\Phi(X) = X^n - 1$ e

$$\Phi_n(X) = \prod_{\substack{1\leq k<n \\ \text{mdc}(k,n)=1}} (X - \omega^k).$$

□

A proposição a seguir mostra como estabelecer alguns itens do teorema acima sem o auxílio de polinômios sobre $\mathbb{Z}_p$.

Proposição 17. *Para cada $n \in \mathbb{N}$, seja*

$$\Phi_n(X) = \prod_{\substack{1\leq k\leq n \\ \text{mdc}(k,n)=1}} (X - \omega_n^k),$$

onde $\omega_n = \text{cis}\,\frac{2\pi}{n}$. Então:

(a) $X^n - 1 = \prod_{0<d|n} \Phi_d(X)$.

(b) Φ_n *é mônico de coeficientes inteiros e grau* $\varphi(n)$.

(c) $\Phi_n(0) = 1$ *para* $n > 1$.

[3]Ver [3].

PROVA.
(a) Basta ver que

$$\begin{aligned}\prod_{0<d|n}\Phi_d(X) &= \prod_{0<d|n}\prod_{\substack{1\leq k\leq d\\ \mathrm{mdc}(k,d)=1}}(X-\omega_d^k) = \prod_{0<d|n}\prod_{\substack{1\leq k\leq n/d\\ \mathrm{mdc}(k,n/d)=1}}(X-\omega_n^{dk})\\ &= \prod_{t=0}^{n-1}(X-\omega_n^t) = X^n-1.\end{aligned}$$

(b) Façamos indução sobre $n\geq 1$ para provar que Φ_n é mônico de coeficientes inteiros. $\Phi_1(X)=X-1$, mônico e de coeficientes inteiros. Suponha que já provamos que a afirmativa é verdadeira para todos os naturais menores que um certo n. Então

$$\Phi(X)=\prod_{\substack{0<d|n\\ d<n}}\Phi_d(X)$$

é mônico de coeficientes inteiros. Como $X^n-1=\Phi_n(X)\Phi(X)$, segue do algoritmo da divisão para polinômios que Φ_n é mônico de coeficientes inteiros. Por fim, note que o grau de Φ_n é igual ao número de inteiros k tais que $1\leq k\leq n$ e $\mathrm{mdc}\,(k,n)=1$. Este número é exatamente $\varphi(n)$.

(c) Façamos nova indução sobre $n>1$. Se $n=2$ então $\Phi_1(X)\Phi_2(X)=X^2-1$, donde $\Phi_2(X)=X+1$ e daí $\Phi_2(0)=1$. Suponha que já provamos que $\Phi_k(0)=1$ para todo inteiro k tal que $2\leq k<n$. Como

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

temos, fazendo $X=0$, que

$$-1=(-1)\Phi_n(0)\prod_{\substack{d|n\\ 1<d<n}}\Phi_d(0)=-\Phi_n(0),$$

e segue que $\Phi_n(0)=1$. □

OBSERVAÇÃO. Não podemos concluir diretamente que o polinômio Φ_n da proposição acima coincide com o $n-$ésimo polinômio ciclotômico porque tal proposição não garante que Φ_n é irredutível sobre $\mathbb{Q}$.

Um famoso teorema de Dirichlet afirma que se em uma progressão aritmética o primeiro termo e a razão forem inteiros positivos relativamente primos então a progressão contém uma infinidade de números primos dentre seus termos. Como aplicação das idéias acima vamos demonstrar um caso especial deste teorema, quando o termo inicial da progressão for igual a 1.

Teorema 18 (Dirichlet - caso particular). *Se $n > 1$ é um inteiro então a progressão aritmética $1, 1+n, 1+2n, \ldots$ contém infinitos números primos.*

PROVA. Sejam $p_1, \ldots, p_k$ primos quaisquer e Φ_n o $n-$ésimo polinômio ciclotômico. Como Φ_n é mônico, podemos escolher um inteiro y tal que $\Phi_n(ynp_1 \ldots p_k) > 1$. Agora, fazendo $a = ynp_1 \ldots p_k$ temos, módulo $ynp_1 \ldots p_k$, que

$$\Phi_n(a) = \Phi_n(ynp_1 \ldots p_k) \equiv \Phi_n(0) = 1\,(mod.\, ynp_1 \ldots p_k).$$

Seja então $\Phi_n(a) = ynp_1 \ldots p_k + 1$. Se p for um fator primo de $\Phi_n(a)$ temos que $p \neq p_1, \ldots, p_k$. Se provarmos que $p \equiv 1\,(mod.\, n)$ teremos terminado. Para tanto, note que mdc $(p, a) = 1$, de modo que faz sentido denotarmos $t = ord_p(a)$. Como $p \mid \Phi_n(a)$ e $\Phi_n(a)$ divide $a^n - 1$, vem que $a^n \equiv 1\,(mod.\, p)$, e daí $t \mid n$. Se mostrarmos que $t = n$ teremos das propriedades da ordem e de $a^{p-1} \equiv 1\,(mod.\, p)$ que $n \mid (p-1)$, e daí $p \equiv 1\,(mod.\, n)$.

Seja $c = a + p$. Temos $c^t - 1 \equiv 0\,(mod.\, p)$. Além disso,

$$c^t - 1 = \prod_{0<d|t} \Phi_d(c).$$

Daí, se $t < n$, temos

$$\begin{aligned} c^n - 1 &= \prod_{0<d|n} \Phi_d(c) = \Phi_n(c) \prod_{\substack{0<d|n \\ d<n}} \Phi_d(c) = \Phi_n(c) \prod_{0<d|t} \Phi_d(c) H(c) \\ &= \Phi_n(c)(c^t - 1)H(c) \equiv 0\,(mod.\, p^2), \end{aligned}$$

uma vez que $c \equiv a (mod.\, p) \Rightarrow \Phi_n(c) \equiv \Phi_n(a) \equiv 0 (mod.\, p)$ (aqui, $H \in \mathbb{Z}[X]$ é algum polinômio apropriado). Por outro lado, módulo p^2 temos

$$0 \equiv c^n - 1 = (a+p)^n - 1 = a^n - 1 + \sum_{j=1}^{n-1} a^j p^{n-j} \binom{n}{j} \equiv n a^{n-1} p,$$

o que é um absurdo por serem a e n relativamente primos com p. Logo, $t = n$. □

Para aprender mais sobre corpos e polinômios ciclotômicos, veja [1] ou [4].

Referências

[1] Endler, Otto. *Teoria dos Corpos*. Monografias de Matemática nº 44. Rio de Janeiro: IMPA, 1987.

[2] Garcia, Arnaldo. & Lequain, Yves. *Elementos de Álgebra*. Rio de Janeiro: IMPA, 2002.

[3] Moreira, C. Gustavo. *Divisibilidade, congruências e aritmética módulo n.*. Eureka 2, 41-53.

[4] Lang, Serge. *Algebra*. Reading: Addison Wesley, 1997.

[5] Santos, A. Plínio dos. *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 1998.