Polinômios Ciclotômicos em Teoria dos Números

Rafael Kazuhiro Miyazaki

26 e 27 de Janeiro de 2018

Esse material é baseado fortemente no artigo Cyclotomic Polynomials in Olympiad Number Theory[1], de Lawrence Sun.

1 Definições Introdutórias

Aqui começamos com as definições que serão, utilizadas como instrumento ao longo do artigo.

Definição 1.1. (Raízes da unidade) Dado um inteiro positivo n, um número complexo z é chamado uma raíz n-ésima da unidade se satisfaz a equação $z^n = 1$. Se n é o menor inteiro positivo para o qual isso é verdade, então z é uma raíz **primitiva** n-ésima da unidade.

Definição 1.2. Dado um inteiro positivo n, definimos $\omega_n = \exp\left(\frac{2\pi i}{n}\right)$, a raíz n-ésima da unidade de menor argumento.

Definição 1.3. (Ordem módulo p) Denotamos por $ord_p(a)$, e chamamos ordem de a módulo p, o menor inteiro positivo k, para o qual $a^k \equiv 1 \pmod{p}$.

2 Introdução à Polinômios Ciclotômicos

Introduzimos agora a definição de polinômios ciclotômicos e alguns teoremas básicos sobre os mesmos.

Definição 2.1. (Polinômio Ciclotômico) Dado um inteiro positivo n, o n-ésimo polinômio ciclotômico é o polinômio mônico cujas raízes são simples e raízes primitivas da unidade, isto é, o polinômio:

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ mdc(k,n)=1}} (x - \omega_n^k).$$

Da definição de polinômios ciclotômicos, podemos tirar algumas importantes conclusões:

Teorema 2.2. Para todo inteiro positivo n, temos $\partial(\Phi_n(x)) = \phi(n)$.

Teorema 2.3. Para todo inteiro positivo n, temos $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Teorema 2.4. Para todo inteiro positivo n, $\Phi_n(x)$ é um polinômio irredutível, simétrico, e de coeficientes inteiros.

Obs: $\Phi_n(x)$ é um polinômio irredutível para todo n inteiro, faremos mais adiante utilizando alguns resultados ainda não mencionados.

3 Propriedades dos Polinômios Ciclotômicos

Definição 3.1. (Função de Möbius) A função de Möbius μ é definida para todo inteiro positivo n da seguinte maneira:

$\mu(n) = 1$, se n é livre de quadrados e tem um número par de divisores primos
$\mu(n) = -1$, se n é livre de quadrados e tem um número ímpar de divisores primos
$\mu(n) = 0$, se n não é livre de quadrados

Teorema 3.2. Para todo inteiro positivo $n > 1$, $\sum_{d|n} \mu(d) = 0$.

Teorema 3.3. (Fórmula de Inversão de Möbius) Sejam f e g duas funções definidas nos números naturais, satisfazendo $g(n) = \sum_{d|n} f(d)$, para todo inteiro positivo n, então $f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$.

Teorema 3.4. Para todo inteiro positivo n, temos $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$.

Teorema 3.5. Para todo inteiro positivo n, a soma das raízes primitivas n-ésimas da unidade é $\mu(n)$.

Teorema 3.6. Seja n um inteiro positivo e p um número primo. Então se $p|n$, temos que $\Phi_{np}(x) = \Phi_n(x^p)$. Se $p \nmid n$, temos que $\Phi_{np}(x) = \dfrac{\Phi_n(x^p)}{\Phi_n(x)}$.

Teorema 3.7. Se a, n são inteiros positivos e $mdc(a, n) = 1$, temos que $\Phi_n(x^a) = \prod_{d|a} \Phi_{nd}(x)$.

Teorema 3.8. Seja P um polinômio em $\mathbb{R}[x]$(ou $\mathbb{Q}[x]$, $\mathbb{Z}[x]$, $\mathbb{Z}_p[x]$). Então existe um polinômio não constante $q(x)$ tal que $q(x)^2 \mid P(x)$ se, e somente se, $\gcd(P(x), P'(x)) \neq 1$.

Teorema 3.9. (Lema de Gauss) Seja $f(x)$ um polinômio mônico de coeficientes inteiros, e suponha que $f(x) = g(x)h(x)$, onde $g(x)$ e $h(x)$ são polinômios mônicos de coeficientes racionais. Então $g(x)$ e $h(x)$ são polinômios de coeficientes inteiros.

Enfim temos as ferramentas necessárias para provar:

Teorema 3.10. Para todo inteiro positivo n, $\Phi_n(x)$ é irredutível em $\mathbb{Z}[x]$.

4 Polinômios Ciclotômicos e Teoria dos Números

Nesta seção, começamos a traduzir para Teoria dos Números alguns resultados de polinômios ciclotômicos.

Proposição 4.1. Sejam m, n inteiros positivos e p um primo tal que $p \nmid mn$. Então $mdc(\Phi_m(x), \Phi_n(x)) = 1$ em $\mathbb{Z}_p[x]$.

Teorema 4.2. Seja p um número primo. Então para todos inteiros positivos n e inteiros a tais que $mdc(n, p) = 1$, temos $p \mid \Phi_n(a) \iff ord_p(a) = n$.

Teorema 4.3. Sejam m, n inteiros positivos distintos e h um inteiro. Então, se

$$mdc(\Phi_m(h), \Phi_n(h)) \neq 1,$$

este valor é p^z e $\dfrac{m}{n} = p^k$, para inteiros z e k, e um primo p.

Teorema 4.4. (Dirichilet para resto 1) Para todo inteiro positivo n, existem infinitos primos da forma $nk + 1$, k inteiro.

5 Teorema de Zsigmondy

Começamos essa seção enunciando o poderoso Teorema de Zsigmondy

Teorema 5.1. (Zsigmondy) Sejam a, b e n inteiros positivos, tais que $a > b > 0, n > 0$, $mdc(a, b) = 1$. Então existe um número primo q divisor de $a^n - b^n$ tal que $q \nmid a^k - b^k$ para todo inteiro k, $0 < k < n$, exceto os seguintes casos:
(1) $n = 1, a - b = 1$
(2) $n = 2, a + b = 2^t$
(3) $n = 6, a = 2, b = 1$

Para isso, podemos provar as seguintes proposições:

Proposição 5.2. Sejam $a, n > 1$ inteiros. Suponha que todos os fatores primos de $\Phi_n(a)$ sejam divisores de n. Então $\Phi_n(a)$ é um primo que divide n, ou $n = 2$.

Proposição 5.3. Sejam $a, n > 1$ inteiros. Escreva $n = p^k r$, onde $p \nmid r$. Então, temos $\Phi_n(a) > (b^{p-2}(b-1))^{\phi(r)}$, onde $b = a^{p^{k-1}}$.

6 Problemas

Problema 1 (BMO)**.** Prove que não existem primos na sequência infinita

$$10001, 100010001, 1000100010001, ...$$

Problema 2 (Japão)**.** Encontre todas as quinas de inteiros positivos (a, n, p, q, r), tais que $a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$.

Problema 3 (WOOT)**.** Seja n um inteiro positivo. Prove que o número $2^{2^n} + 2^{2^{n-1}} + 1$ pode ser escrito como o produto de não menos que n fatores primos (não necessariamente distintos).

Problema 4. Prove que existem infinitos inteiros positivos n, tais que todos os divisores primos de $n^2 + n + 1$ não são maiores que $\sqrt{n}$.

Problema 5. Prove a existência de raízes primitivas módulo p, para todo p primo.

Problema 6 (OMO)**.** ω é um número complexo tal que $\omega^{2013} = 1$ e $\omega^m \neq 1$ para $m = 1, 2, \ldots, 2012$. Encontre o número de pares ordenados de inteiros (a, b), com $1 \leq a, b \leq 2013$ tais que

$$\frac{(1 + \omega + \cdots + \omega^a)(1 + \omega + \cdots + \omega^b)}{3}$$

é raíz de algum polinômio com coeficientes inteiros e coeficiente líder 1(isto é, um inteiro algébrico).

Problema 7 (IMO)**.** Se p é um número primo, mostre que existe um outro número primo q tal que $n^p - p$ não é um múltiplo de q para nenhum natural n.

Problema 8. Encontre todas as soluções inteiras positivas da seguinde igualdade:

$$(a + 1)(a^2 + a + 1) \cdots (a^n + a^{n-1} + \cdots + 1) = (a^m + a^{m-1} + \cdots + 1).$$

Problema 9. Sejam $p_1, p_2, \cdots, p_k$ primos distintos maiores que 3, e seja $N = 2^{p_1 p_2 \cdots p_k} + 1$. Mostre que N tem pelo menos $2^{2^{k-1}}$ divisores.

7 Bibliografia

[1]Cyclotomic Polynomials in Olympiad Number Theory(2013). Lawrence Sun. PDF encontrado em: https://services.artofproblemsolving.com/download.php?id=YXR0YWNobWVudHMvYy84LzMxZGEwZGU0MWYzYWQ3Y
rn=Q3ljbG90b21pYyBQb2x5bm9taWFscy5wZGY=