Material Teórico - Módulo Aritmética dos Restos

Raízes primitivas e uma generalização do Teorema de Wilson – Parte 1

Tópicos Adicionais

Autor: Ulisses Lima Parente
Revisor: Prof. Antonio Caminha M. Neto

20 de janeiro de 2024

Nas duas últimas aulas deste módulo, caracterizaremos os inteiros positivos n para os quais existe uma *raiz primitiva módulo n*. Mais precisamente, mostraremos que se $n > 1$ é um inteiro, então existe raiz primitiva módulo n se, e somente se, $n = 2, 4, p^k$ ou $2p^k$, em que p é um primo ímpar. Além disso, apresentaremos, como aplicação, uma generalização do Teorema de Wilson. Antes, porém, necessitamos de alguns resultados preliminares.

Iniciamos esta aula lembrando que se $a \neq 0$ e $n > 1$ são inteiros relativamente primos, então a *ordem de a, módulo n*, é o menor inteiro $k \geq 1$ tal que $a^k \equiv 1 \pmod{n}$; em particular, a é uma raiz primitiva módulo n quando $\mathrm{ord}_n(a) = \phi(n)$. No encerramento da aula anterior, provamos a seguinte proposição.

Proposição 1. *Sejam $a \neq 0$ e $n > 1$ inteiros relativamente primos. Se $\mathrm{ord}_n(a) = d$, então os inteiros $1, a, a^2, \ldots, a^{d-1}$ são dois a dois incongruentes, módulo n. Em particular, se a é uma raiz primitiva módulo n, então $\{1, a, a^2, \ldots, a^{\phi(n)-1}\}$ é um sistema reduzido de resíduos, módulo n.*

A partir de agora, passamos a apresentar uma sequência de resultados importantes, os quais serão utilizados para provar o resultado central deste material. Como corolário de um desses resultados, reobteremos o Teorema de Wilson, que foi provado de modo diferente na aula anterior.

Proposição 2. *Sejam n, k e a inteiros, tais que $n > 1$, $k > 0$ e $\mathrm{mdc}(n,a) = 1$. Então,*

$$\mathrm{ord}_n(a) = \mathrm{mdc}\,(\mathrm{ord}_n(a), k) \cdot \mathrm{ord}_n(a^k).$$

Em particular,

$$\mathrm{ord}_n(a) = \mathrm{ord}_n\left(a^k\right) \iff \mathrm{mdc}\,(\mathrm{ord}_n(a), k) = 1.$$

Prova. Sejam $p = \mathrm{ord}_n(a)$, $q = \mathrm{ord}_n\left(a^k\right)$ e $d = \mathrm{mdc}\,(p,k)$. Devemos mostrar que $p = dq$. De fato, $q = \mathrm{ord}_n\left(a^k\right)$ é o menor elemento do conjunto

$$A = \{m \in \mathbb{Z} | m > 0 \text{ e } \left(a^k\right)^m \equiv 1 \pmod{n}\}.$$

Mas veja que $m \in A$ se, e somente se, m é inteiro positivo e

$$\begin{aligned} a^{mk} = \left(a^k\right)^m \equiv 1 \,(\mathrm{mod}\, n) &\iff \mathrm{ord}_n(a) = p \mid mk \\ &\iff mk \equiv 0 \,(\mathrm{mod}\, p) \\ &\iff m \cdot \frac{k}{d} \equiv 0 \,\left(\mathrm{mod}\, \frac{p}{d}\right) \\ &\iff m \equiv 0 \,\left(\mathrm{mod}\, \frac{p}{d}\right). \end{aligned}$$

A última equivalência foi possível porque $d = \mathrm{mdc}\,(p,k) \Rightarrow \mathrm{mdc}\left(\frac{p}{d}, \frac{k}{d}\right) = 1$. Portanto,

$$\begin{aligned} A &= \left\{ m \in \mathbb{Z} | m > 0 \text{ e } m \equiv 0 \,\left(\mathrm{mod}\, \frac{p}{d}\right)\right\} \\ &= \left\{ \frac{p}{d}, \frac{2p}{d}, \frac{3p}{d}, \cdots \right\}. \end{aligned}$$

Daí, segue que o menor elemento de A é igual a $\frac{p}{d}$. Por outro lado, como q também é o menor elemento de A, temos $q = \frac{p}{d}$, ou seja, $p = dq$. □

Proposição 3. *Seja $n > 1$ inteiro. Se a é uma raiz primitiva módulo n, então qualquer raiz primitiva módulo n é congruente a um dos elementos do conjunto*

$$\{a^k | \, 1 \leq k \leq \phi(n) \;\; e \;\; \mathrm{mdc}\;(\phi(n),k) = 1\}.$$

Em particular, há exatamente $\phi\,(\phi(n))$ raízes primitivas módulo n.

Prova. Seja a uma raiz primitiva módulo n, de sorte que $\mathrm{mdc}\,(a,n) = 1$ e $\mathrm{ord}_n(a) = \phi(n)$. Pela proposição 1, temos que $\{1,a,\ldots,a^{\phi(n)-1}\}$ é um sistema reduzido de resíduos módulo n, logo (uma vez que $\mathrm{mdc}\,(a,n) = 1$), $\{a,a^2,\ldots,a^{\phi(n)}\}$ também é um sistema reduzido de resíduos módulo n. Portanto, qualquer raiz primitiva módulo n deve ser congruente a alguma potência a^k, com $k \in \{1,2,\ldots,n\}$.

Por outro lado, pela proposição 2, temos que

$$\mathrm{ord}_n\left(a^k\right) = \mathrm{ord}_n(a) = \phi(n) \iff \mathrm{mdc}\,(\phi(n),k) = 1.$$

Assim, a^k será raiz primitiva se, e só se, mdc $(\phi(n),k) = 1$.

Daí, concluímos que qualquer raiz primitiva módulo n é congruente a um dos elementos do conjunto

$$\{a^k | \, 1 \leq k \leq \phi(n) \text{ e mdc } (\phi(n),k) = 1\}.$$

Para o que falta, note que a quantidade de elementos do conjunto $\{a^k | \, 1 \leq k \leq \phi(n)$ e mdc $(\phi(n),k) = 1\}$ é igual à quantidade de elementos do conjunto $\{k \in \mathbb{Z} | \, 1 \leq k \leq \phi(n)$ e mdc $(\phi(n),k) = 1\}$, mas essa última quantidade é precisamente $\phi(\phi(n))$. □

Proposição 4. *Se n é um inteiro positivo, então*

$$\sum_{0<d|n} \phi(d) = n.$$

Prova. Seja D_n o conjunto dos divisores positivos de n. Para cada $d \in D_n$, considere o conjunto

$$A_d = \{m \in \mathbb{Z} | \, 1 \leq m \leq n \text{ e mdc}\,(m,n) = d\}.$$

Veja que, se m é um inteiro tal que $1 \leq m \leq n$ e $d =$ mdc (m,n), então $m \in A_d$. Logo,

$$\bigcup_{d \in D_n} A_d = \{1,2,\ldots,n\}.$$

Ademais, a união acima é disjunta, uma vez que, fixado um inteiro $1 \leq m \leq n$, o número mdc (m,n) assume um único valor. Desse modo,

$$\sum_{d \in D_n} n\,(A_d) = n\,(\{1,2,\ldots,n\}) = n, \tag{1}$$

em que $n\,(A_d)$ é a quantidade de elementos de A_d.

Para calcular $n(A_d)$ quando d é um divisor comum de m e n, note que mdc $(m,n) = d$ se, e somente se, mdc $\left(\frac{m}{d},\frac{n}{d}\right) = 1$. Assim,

$$\begin{aligned} A_d &= \{m \in \mathbb{Z} | \, 1 \leq m \leq n \text{ e mdc } \left(\frac{m}{d},\frac{n}{d}\right) = 1\} \\ &= \{k \in \mathbb{Z} | \, 1 \leq k \leq \frac{n}{d} \text{ e mdc } \left(k,\frac{n}{d}\right) = 1\}, \end{aligned}$$

de onde concluímos que

$$n\left(A_d\right) = \phi\left(\frac{n}{d}\right). \tag{2}$$

Para finalizar, note que a função $f : D_n \longrightarrow D_n$ definida por $f(d) = \frac{n}{d}$ é uma bijeção (quando d varia de 1 a n, percorrendo os divisores positivos de n, então $\frac{n}{d}$ varia de n a 1, mas também percorre todos os divisores positivos de n). Logo,

$$\sum_{d\in D_n} \phi(d) = \sum_{d\in D_n} \phi\left(\frac{n}{d}\right). \tag{3}$$

Então, segue de (1), (2) e (3) que

$$\sum_{d\in D_n} \phi(d) = \sum_{d\in D_n} \phi\left(\frac{n}{d}\right) = \sum_{d\in D_n} n\left(A_d\right) = n.$$

□

Teorema 5 (Lagrange). *Sejam p primo e $f(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ um polinômio com coeficientes inteiros tal que $p \nmid c_n$. Então, a congruência $f(x) \equiv 0 \pmod p$ possui, no máximo, n soluções duas a duas incongruentes módulo p.*

Prova. Faremos indução sobre n.

Para $n = 1$, o resultado é verdadeiro, pois, como vimos em aulas anteriores, a congruência linear $c_1 x \equiv -c_0 \pmod p$ possui exatamente uma solução módulo p, uma vez que $\text{mdc}\,(c_1, p) = 1 \mid c_0$.

Vamos admitir que que o resultado seja verdadeiro para todo polinômio de grau $n-1$ e supor, por contradição, que exista $f(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$, polinômio com coeficientes inteiros tal que $p \nmid c_n$ e $f(x) \equiv 0 \pmod p$ possui ao menos $n+1$ soluções duas a duas incongruentes módulo p

Sendo x_0, x_1, …, x_n tais soluções, considere o polinômio $g(x) = f(x) - f(x_0)$, que também tem grau n. Escrevendo

$$x^j - x_0^j = (x - x_0)\left(x^{j-1} + x^{j-2}x_0 + \ldots + x x_0^{j-2} + x_0^{j-1}\right)$$

para $j \in \{2,\ldots,n\}$, obtemos

$$\begin{aligned} g(x) &= f(x) - f(x_0) \\ &= \left(c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0\right) \\ &\quad - \left(c_n x_0^n + c_{n-1}x_0^{n-1} + \ldots + c_1 x_0 + c_0\right) \\ &= c_n\left(x^n - x_0^n\right) + c_{n-1}\left(x^{n-1} - x_0^{n-1}\right) \\ &\quad + \ldots + c_1\left(x - x_0\right) \\ &= (x - x_0)\, h(x), \end{aligned}$$

em que $h(x)$ é um polinômio de grau $n-1$ que tem c_n como coeficiente de x^{n-1}. Mas veja que, para todo $j \in \{1,2,\ldots,n\}$, temos

$$(x_j - x_0)\, h(x_j) = g(x_j) = f(x_j) - f(x_0) \equiv 0 \,(\mathrm{mod}\, p)$$

e, como as soluções x_0, x_1, ..., x_n são duas a duas incongruentes módulo p, temos que $\mathrm{mdc}\,(p, x_j - x_0) = 1$, donde concluímos que $h(x_j) \equiv 0 \,(\mathrm{mod}\, p)$, $\forall j \in \{1,2,\ldots,n\}$. Isso é uma contradição, pois estamos admitindo o resultado verdadeiro para $n-1$. □

Teorema 6. *Sejam p primo e $f(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ um polinômio de grau n com coeficientes inteiros. Se a congruência $f(x) \equiv 0 \,(\mathrm{mod}\, p)$ tiver mais do que n soluções, então todos os coeficientes de f são divisíveis por p.*

Prova. Suponhamos que algum coeficiente de $f(x)$ não seja divisível por p. Seja j o maior elemento de

$$\{k \in \mathbb{Z} |\, 0 \leq k \leq n \text{ e } p \nmid c_k\}.$$

Então $p \mid c_k$ para $j < k \leq n$ e, assim, se x é solução de $f(x) \equiv 0 \,(\mathrm{mod}\, p)$, então x é solução de

$$c_j x^j + c_{j-1}x^{j-1} + \ldots + c_1 x + c_0 \equiv 0 \,(\mathrm{mod}\, p).$$

Desse modo, a última congruência acima tem mais do que n soluções. Por outro lado, como $p \nmid c_j$, o Teorema de Lagrange garante que a quantidade de soluções dessa congruência é no máximo $j \leq n$, o que é uma contradição. Portanto, todos os coeficientes de $f(x)$ são divisíveis por p. □

Teorema 7. *Se p é primo, então p divide todos os coeficientes do polinômio*

$$f(x) = (x-1)(x-2)\dots(x-p+1) - x^{p-1} + 1.$$

Prova. Podemos escrever $f(x) = g(x) - h(x)$, em que $g(x) = (x-1)(x-2)\dots(x-p+1)$ e $h(x) = x^{p-1} - 1$. Perceba que $f(x)$ tem grau $p-2$.

Agora, veja que os números inteiros $1,2,\dots,p-1$ são soluções de $g(x) \equiv 0 \pmod p$, pois são raízes de $g(x)$. Por outro lado, como cada um dos números $1,2,\dots,p-1$ é relativamente primo com p, o Pequeno Teorema de Fermat garante que cada um desses números também é solução de $h(x) = x^{p-1} - 1 \equiv 0 \pmod p$. Logo, cada um desses $p-1$ números, que são dois a dois incongruentes módulo p, é solução de $f(x) = g(x) - h(x) \equiv 0 \pmod p$. Pelo teorema 6, concluímos que os coeficientes de $f(x)$ são todos divisíveis por p. □

Corolário 8. *Se p é primo, então*

$$(p-1)! \equiv -1 \pmod p.$$

Prova. Se $p = 2$, isso é imediato. Se $p > 2$, basta notar que o termo independente de x no polinômio $f(x)$ do teorema 7 é igual a $(p-1)! + 1$ (pois $(-1)^{p-1} = 1$). □

Teorema 9. *Sejam p um primo ímpar e d um divisor positivo de $p-1$. Então, existem exatamente $\phi(d)$ inteiros pertencentes ao conjunto $\{1,2,\dots,p-1\}$, cujas ordens módulo p são iguais a d. Em particular, há exatamente $\phi(p-1)$ raízes primitivas módulo p, duas a duas incongruentes módulo p.*

Prova. Como na demonstração da proposição 4, D_{p-1} denota o conjunto dos divisores positivos de $p-1$.

Para cada $d \in D_{p-1}$, seja

$$A_d = \{m \in \mathbb{Z} \mid 1 \le m \le p-1 \text{ e } \operatorname{ord}_p(m) = d\}.$$

Veja que, pelo Teorema de Fermat, $m^{p-1} \equiv 1 \pmod p$, $\forall m \in \{1,2,\dots,p-1\}$, logo, $\operatorname{ord}_p(m) \mid (p-1)$, $\forall m \in \{1,2,\dots,p-1\}$.

Desse modo, se $m \in \{1,2,\ldots,p-1\}$, então $m \in A_d$, em que $d = \mathrm{ord}_p(m) \mid (p-1)$. Portanto, podemos escrever

$$\bigcup_{d \in D_{p-1}} A_d = \{1,2,\ldots,p-1\},$$

o que acarreta

$$\sum_{d \in D_{p-1}} n\left(A_d\right) = n\left(\{1,2,\ldots,p-1\}\right) = p-1,$$

pois a união na igualdade de conjuntos acima é disjunta. Por outro lado, utilizando a proposição 4, obtemos

$$\sum_{d \in D_{p-1}} \phi(d) = p-1 = \sum_{d \in D_{p-1}} n\left(A_d\right). \tag{4}$$

Agora, suponha que A_d seja não vazio e tome $a \in A_d$. Pela proposição 1, obtemos que $1,a,\ldots,a^{d-1}$ são dois a dois incongruentes módulo p, logo (uma vez que $\mathrm{mdc}\,(a,p) = 1$), $a,a^2,\ldots,a^d$ também são dois a dois incongruentes módulo p. O teorema 5 garante que $x^d \equiv 1 \pmod p$ possui, no máximo, d soluções incongruentes módulo p. Além disso, cada um dos d inteiros $a,a^2,\ldots,a^d$ é solução dessa congruência, pois $d^d \equiv 1 \pmod p$. Daí, $a,a^2,\ldots,a^d$ são todas as soluções da congruência $x^d \equiv 1 \pmod p$. Assim, cada elemento de A_d é congruente a alguma potência a^k, $k \in \{1,2,\ldots,d\}$. Mas a proposição 2 nos diz que $\mathrm{ord}_p\left(a^k\right) = \mathrm{ord}_p(a)$ se, e somente se, $\mathrm{mdc}\,(d,k) = 1$. Assim, cada elemento de A_d é congruente a um, e somente um, elemento do conjunto $\{a^k | 1 \leq k \leq d \text{ e } \mathrm{mdc}\,(d,k) = 1\}$, donde concluímos que $n\left(A_d\right) = \phi(d)$.

Portanto, para cada $d \in D_{p-1}$, temos $n(A_d) = 0$ (se $A_d = \emptyset$) ou $n\left(A_d\right) = \phi(d)$ (se $A_d \neq \emptyset$). Então, segue de (4) que $n\left(A_d\right) = \phi(d)$ para todo $d \in D_{p-1}$. □

Dicas para o Professor

Sugerimos que sejam utilizadas três sessões de 50min para expor o conteúdo deste material. Antes de iniciar a aula, recomendamos uma breve revisão sobre os conceitos de ordem e raiz primitiva módulo n. Também é interessante relembrar os resultados apresentados na aula anterior e que serão utilizados para provar resultados apresentados nesta aula.

Sugestões de Leitura Complementar

1 A. C. Muniz Neto. *Tópicos de Matemática Elementar, Volume 5: Teoria dos Números*, terceira edição. Rio de Janeiro, SBM, 2022.

2. J. P. O. Santos *Introdução à Teoria dos Números*. IMPA, 2000.