Material Teórico - Módulo Aritmética dos Restos

Raízes primitivas e uma generalização do Teorema de Wilson – Parte 2

Tópicos Adicionais

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

20 de Fevereiro de 2024

PORTAL DA MATEMÁTICA
OBMEP

Este material finaliza o módulo de Aritmética dos restos. Nele, caracterizaremos os inteiros positivos que possuem raízes primitivas e, como aplicação, provaremos uma generalização do Teorema de Wilson.

Como $1^1 \equiv 1 \pmod 2$, $\phi(2) = 1$, $3^1 \equiv 3 \pmod 4$, $3^2 \equiv 1 \pmod 4$ e $\phi(4) = 2$, concluímos que 1 é raiz primitiva módulo 2 e 3 é raiz primitiva módulo 4. A seguinte sequência de resultados mostra que existem raízes primitivas módulo n quando $n = p^k$ ou $2p^k$, em que p é um primo ímpar e k é um inteiro positivo.

Proposição 1. *Sejam a e $n > 1$ inteiros relativamente primos. Então*

$$\mathrm{ord}_n(a+n) = \mathrm{ord}_n(a).$$

Prova. Veja que $\mathrm{mdc}\,(a+n,n) = \mathrm{mdc}\,(a,n) = 1$ e, como $a + n \equiv a \pmod n$, temos que $(a+n)^k \equiv a^k \pmod n$, para todo k inteiro positivo. Denotemos $d_1 = \mathrm{ord}_n(a)$ e $d_2 = \mathrm{ord}_n(a+n)$.

- Como $a^{d_2} \equiv (a+n)^{d_2} \equiv 1 \pmod n$, a definição de $\mathrm{ord}_n(a)$ garante que $d_1 \leq d_2$.
- Como $(a+n)^{d_1} \equiv a^{d_1} \equiv 1 \pmod n$, a definição de $\mathrm{ord}_{a+n}(a)$ garante que $d_2 \leq d_1$.

Então, $d_1 = d_2$, como queríamos provar. □

Teorema 2. *Se p é primo ímpar, então existe uma raiz primitiva módulo p.*

Prova. Na aula anterior, provamos que se p é um primo ímpar e d é um inteiro positivo tal que $d \mid (p-1)$, então há $\phi(d)$ inteiros pertencentes ao conjunto $\{1,2,\ldots,p-1\}$ cujas ordens módulo p são iguais a d. Em particular, fazendo $d = p-1$, há $\phi(p-1)$ inteiros pertencentes a $\{1,2,\ldots,p-1\}$ cujas ordens módulo p são iguais a $d = p-1 = \phi(p)$, ou seja, há $\phi(p-1)$ raízes primitivas módulo p. □

Proposição 3. *Se p é um primo ímpar, então existe a, raiz primitiva módulo p, tal que*

$$a^{p-1} \not\equiv 1 \pmod{p^2}.$$

Prova. O teorema 2 garante que se p é um primo ímpar, então existe raiz primitiva módulo p. Vamos denotar essa raiz primitiva por a.

Se a satisfizer $a^{p-1} \not\equiv 1 \pmod{p^2}$, nada há a fazer. Assim, suponha que $a^{p-1} \equiv 1 \pmod{p^2}$. Pela proposição 1, temos que $\mathrm{ord}_p(a+p) = \mathrm{ord}_p(a) = \phi(p)$, logo, $a+p$ também é raiz primitiva módulo p. Mostraremos que $(a+p)^{p-1} \not\equiv 1 \pmod{p^2}$. De fato, veja que

$$\begin{aligned}(a+p)^{p-1} &= \sum_{i=0}^{p-1} \binom{p-1}{i} a^{p-1-i} p^i \\ &= a^{p-1} + (p-1)a^{p-2}p + \sum_{i=2}^{p-1} \binom{p-1}{i} a^{p-1-i} p^i.\end{aligned}$$

Como $p^i \equiv 0 \pmod{p^2}$ sempre que $i \geq 2$, segue da última expressão acima que

$$(a+p)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}p \pmod{p^2}.$$

Uma vez que $(p-1)a^{p-2}p = p^2a^{p-2} - pa^{p-2}$, temos que

$$\begin{aligned}(a+p)^{p-1} &\equiv a^{p-1} + p^2a^{p-2} - pa^{p-2} \pmod{p^2} \\ &\equiv 1 - pa^{p-2} \pmod{p^2}.\end{aligned}$$

Desse modo, se tivéssemos $(a+p)^{p-1} \equiv 1 \pmod{p^2}$, então deveríamos ter $pa^{p-2} \equiv 0 \pmod{p^2}$, o que não pode acontecer, pois isso implicaria $p^2 \mid pa^{p-2}$, logo, $p \mid a$; contudo, isso é impossível, já que $\mathrm{mdc}\,(a,p) = 1$ (pois a é raiz primitiva módulo p). Portanto, concluímos que $(a+p)^{p-1} \not\equiv 1 \pmod{p^2}$, como queríamos. □

Teorema 4. *Se p é um primo ímpar e a é uma raiz primitiva módulo p tal que $a^{p-1} \not\equiv 1 \pmod{p^2}$, então*

$$a^{\phi\left(p^{k-1}\right)} \not\equiv 1 \pmod{p^k},$$

para todo inteiro $k \geq 2$.

Prova. Vamos utilizar indução sobre o expoente k. Para $k = 2$, temos

$$\begin{aligned} a^{\phi\left(p^{2-1}\right)} \not\equiv 1 \pmod{p^2} &\iff a^{\phi(p)} \not\equiv 1 \pmod{p^2} \\ &\iff a^{p-1} \not\equiv 1 \pmod{p^2}, \end{aligned}$$

que é verdade, por hipótese.

Agora, supondo que $a^{\phi\left(p^{k-1}\right)} \not\equiv 1 \pmod{p^k}$ para um certo $k \geq 2$, mostraremos que $a^{\phi\left(p^k\right)} \not\equiv 1 \pmod{p^{k+1}}$. Veja que mdc $\left(a,p^{k-1}\right) = 1$, logo, podemos aplicar o Teorema de Euler para obter

$$a^{\phi\left(p^{k-1}\right)} \equiv 1 \pmod{p^{k-1}}.$$

Assim, existe n inteiro tal que

$$a^{\phi\left(p^{k-1}\right)} = 1 + np^{k-1}.$$

Perceba que $p \nmid n$, pois, caso contrário, existiria q inteiro tal que $n = qp$ e, daí,

$$a^{\phi\left(p^{k-1}\right)} = 1 + np^{k-1} = 1 + qp^k \equiv 1 \pmod{p^k},$$

o que contraria a hipótese de indução. Continuando, veja que

$$\begin{aligned} a^{\phi\left(p^{k-1}\right)} = 1 + np^{k-1} &\implies \left(a^{\phi\left(p^{k-1}\right)}\right)^p = \left(1 + np^{k-1}\right)^p \\ &\implies a^{p\phi\left(p^{k-1}\right)} = \left(1 + np^{k-1}\right)^p \\ &\implies a^{\phi\left(p^k\right)} = \left(1 + np^{k-1}\right)^p \end{aligned}$$

e

$$\begin{aligned} \left(1 + np^{k-1}\right)^p &= \sum_{i=0}^{p} \binom{p}{i} \left(np^{k-1}\right)^i \\ &= 1 + pnp^{k-1} + \frac{p(p-1)}{2} n^2 p^{2(k-1)} + \\ &\quad + \sum_{i=3}^{p} \binom{p}{i} \left(np^{k-1}\right)^i \\ &= 1 + np^k + \frac{(p-1)}{2} n^2 p^{2k-1} + S, \end{aligned}$$

em que $S = \sum_{i=3}^{p} \binom{p}{i} \left(np^{k-1}\right)^i$. Mas,

$$k \geq 2 \Longrightarrow 2k-1, 3k-3 \geq k+1.$$

Dessa forma,

$$\frac{(p-1)}{2} n^2 p^{2k-1} \equiv 0 \left(\mathrm{mod}\, p^{k+1}\right)$$

e, para $i \geq 3$,

$$i(k-1) \geq 3(k-1) \geq k+1;$$

portanto, cada parcela da soma S também é divisível por uma potência de p cujo expoente é maior ou igual a $k+1$. Assim,

$$\begin{aligned} a^{\phi(p^k)} &= 1 + np^k + \frac{(p-1)}{2} n^2 p^{2k-1} + S \\ &\equiv 1 + np^k \left(\mathrm{mod}\, p^{k+1}\right). \end{aligned}$$

Uma vez que $p \nmid n$, temos que $p^{k+1} \nmid np^k$, logo, $np^k \not\equiv 0 \left(\mathrm{mod}\, p^{k+1}\right)$ e, consequentemente,

$$a^{\phi\left(p^k\right)} \not\equiv 1 \left(\mathrm{mod}\, p^{k+1}\right),$$

como queríamos. □

Teorema 5. *Sejam p um primo ímpar e a uma raiz primitiva módulo p. Então, a é uma raiz primitiva módulo p^k, qualquer que seja $k \geq 1$ inteiro, se, e somente se, $a^{p-1} \not\equiv 1 \left(\mathrm{mod}\, p^2\right)$.*

Prova. Seja a uma raiz primitiva módulo p, a qual sabemos que existe, pelo teorema 2. Se a também for raiz primitiva módulo p^k, $\forall k \geq 1$ inteiro, então

$$a^{p-1} \not\equiv 1 \left(\mathrm{mod}\, p^2\right),$$

pois $p-1 < p(p-1) = \phi\left(p^2\right) = \mathrm{ord}_{p^2}(a)$.

Reciprocamente, suponha que $a^{p-1} \not\equiv 1 \pmod{p^2}$. Sejam $k \geq 1$ inteiro e $d = \mathrm{ord}_{p^k}(a)$. Devemos mostrar que $d = \phi\left(p^k\right)$. Com efeito, como $a^d \equiv 1 \pmod{p^k}$, temos que $a^d \equiv 1 \pmod{p}$. Daí, $(p-1) \mid d$, pois $p - 1 = \phi(p) = \mathrm{ord}_p(a)$. Assim, existe n inteiro positivo tal que $d = n(p-1)$. Por outro lado, utilizando mais uma vez o teorema de Euler, temos que $a^{\phi\left(p^k\right)} \equiv 1 \pmod{p^k}$, logo, $n(p-1) = d \mid \phi\left(p^k\right)$. Portanto, $n(p-1) \mid p^{k-1}(p-1)$, o que implica $n \mid p^{k-1}$. Assim, $n = p^m$, em que $0 \leq m \leq k-1$. Se $m \leq k-2$, teríamos

$$d = p^m(p-1) \mid p^{k-2}(p-1) = \phi\left(p^{k-1}\right).$$

Daí, $\phi\left(p^{k-1}\right) = qd$, para algum $q \geq 1$ inteiro. Logo,

$$\begin{aligned} a^d \equiv 1 \pmod{p^k} &\Longrightarrow \left(a^d\right)^q \equiv 1^q \pmod{p^k} \\ &\Longrightarrow a^{qd} \equiv 1 \pmod{p^k} \\ &\Longrightarrow a^{\phi\left(p^{k-1}\right)} \equiv 1 \pmod{p^k}. \end{aligned}$$

Como isso contraria o teorema 4, concluímos que $m = k-1$ e $n = p^{k-1}$, donde obtemos

$$d = p^{k-1}(p-1) = \phi\left(p^k\right).$$

□

Teorema 6. *Se p é um primo ímpar, então existe raiz primitiva módulo p^k, em que $k \geq 1$ é um inteiro positivo qualquer.*

Prova. Sejam p um primo ímpar. Pelo teorema 3, existe a raiz primitiva módulo p tal que $a^{p-1} \not\equiv 1 \pmod{p^2}$. Então, pelo teorema 5, a é uma raiz primitiva módulo p^k, $\forall k \geq 1$ inteiro. □

Teorema 7. *Se p é um primo ímpar, então existe raiz primitiva módulo $2p^k$, em que $k \geq 1$ é um inteiro positivo qualquer.*

Prova. Seja a uma raiz primitiva módulo p^k (cuja existência é garantida pelo teorema 6). Utilizando a proposição 1, obtemos $\mathrm{ord}_{p^k}\left(a + p^k\right) = \mathrm{ord}_{p^k}(a) = \phi\left(p^k\right)$, donde concluímos

que $a + p^k$ também é raiz primitiva módulo p^k. Agora, a ou $a + p^k$ é ímpar, logo, existe uma raiz primitiva ímpar módulo p^k.

Assim, vamos admitir, daqui em diante, que a é ímpar. Mostraremos que a também é uma raiz primitiva módulo $2p^k$. Iniciamos observando que $\text{mdc}\left(a,2p^k\right) = 1$, pois a é ímpar e relativamente primo com p^k, já que é raiz primitiva módulo p^k. Seja $d = \text{ord}_{2p^k}(a)$.

Mais uma vez apelando ao Teorema de Euler, temos que $a^{\phi\left(2p^k\right)} \equiv 1 \pmod{2p^k}$, donde concluímos que $d \mid \phi\left(2p^k\right)$. Mas

$$\phi\left(2p^k\right) = \phi(2)\phi\left(p^k\right) = \phi\left(p^k\right),$$

logo, $d \mid \phi\left(p^k\right)$. Por outro lado, como $a^d \equiv 1 \pmod{2p^k}$, temos que $a^d \equiv 1 \pmod{p^k}$ e, como $\text{ord}_{p^k}(a) = \phi\left(p^k\right)$, temos que $\phi\left(p^k\right) \mid d$. Assim, concluímos que $d = \phi\left(p^k\right) = \phi\left(2p^k\right)$, ou seja, a é raiz primitiva módulo $2p^k$. □

Para finalizar a caracterização dos inteiros n para os quais existe raiz primitiva módulo n, precisamos do seguinte teorema.

Teorema 8. *Se $n \geq 2$ é um inteiro positivo diferente de 2, 4, p^k e $2p^k$, em que p é primo ímpar e $k \geq 1$ é inteiro, então não existe raiz primitiva módulo n.*

Prova. Se $n \neq 2$, 4, p^k, $2p^k$, em que p é primo ímpar e $k \geq 1$ é inteiro, então ou (i) $n = 2^k$, com $k \geq 3$, ou (ii) $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, com $r \geq 2$ e $2 \leq p_1 < p_2 < \ldots < p_r$ primos, com $k_1 \geq 2$ se $p_1 = 2$. Analisemos esses dois casos separadamente.

(i) Se $n = 2^k$ e a é um inteiro ímpar, afirmamos que $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. Como $\phi(2^k) = 2^{k-1}$, isso será suficiente para garantir que 2^k não possui raízes primitivas.

Para o que falta, se $k = 3$, então é bem sabido que $a^2 \equiv 1 \pmod{8}$ (veja, por exemplo, a proposição 5.9 de [1]). Admitamos, por hipótese de indução, que $a^{2^{l-2}} \equiv 1 \pmod{2^l}$

para um certo $l \geq 3$, digamos, $a^{2^{l-2}} = 2^l q + 1$, para um certo $q \in \mathbb{N}$. Então,

$$\begin{aligned} a^{2^{l-1}} &= (a^{2^{l-2}})^2 = (2^l q + 1)^2 \\ &= 2^{2l} q^2 + 2^{l+1} q + 1 \\ &= 2^{l+1}(2^{l-1} q^2 + q) + 1 \equiv 1 \,(\mathrm{mod}\, 2^{l+1}), \end{aligned}$$

o que estabelece o passo de indução.

(ii) Seja $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, com $r \geq 2$ e $2 \leq p_1 < p_2 < \dots < p_r$ primos. Suponha, por absurdo, que exista uma raiz primitiva módulo n. Denotemos tal raiz por a. Como $\mathrm{mdc}\,(a,n) = 1$, temos que $\mathrm{mdc}\,\big(a,p_i^{k_i}\big) = 1$, $\forall i \in \{1,2,\dots,r\}$. Outra vez pelo Teorema de Euler, temos que

$$a^{\phi\left(p_i^{k_i}\right)} \equiv 1 \left(\mathrm{mod}\, p_i^{k_i}\right).$$

Assim, denotando $m = \mathrm{mmc}\left(\phi(p_1^{k_1}),\phi(p_2^{k_2}),\dots,\phi(p_r^{k_r})\right)$, temos que $a^m \equiv 1 \left(\mathrm{mod}\, p_i^{k_i}\right)$, $\forall i \in \{1,2,\dots,r\}$, donde obtemos $a^m \equiv 1 \,(\mathrm{mod}\, n)$. Assim, $\phi(n) = \mathrm{ord}_n(a)$ divide m. Mas

$$\phi(n) = \phi\big(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}\big) = \phi\big(p_1^{k_1}\big)\phi\big(p_2^{k_2}\big) \dots \phi\big(p_r^{k_r}\big).$$

Portanto, $m = \phi\big(p_1^{k_1}\big)\phi\big(p_2^{k_2}\big) \dots \phi\big(p_r^{k_r}\big)$, e isso acarreta, pela definição de m como o mmc de $\phi(p_1^{k_1})$, $\phi(p_2^{k_2})$, $\dots$, $\phi(p_r^{k_r})$, que $\mathrm{mdc}\,\big(\phi(p_i^{k_i}),\phi(p_j^{k_j})\big) = 1$ se $i \neq j$. Mas isso é um absurdo, uma vez que

$$\phi\big(p_i^{k_i}\big) = p_i^{k_i - 1}(p_i - 1)$$

é par se p_i for ímpar ou se $i = 1$, $p_1 = 2$ e $k_1 \geq 2$. □

Finalmente, temos condições de provar a seguinte generalização do Teorema de Wilson.

Teorema 9. *Sejam $n \geq 2$ um inteiro positivo que possui raiz primitiva e $1 = a_1 < a_2 < \dots < a_{\phi(n)} = n - 1$ os inteiros de 1 a n e relativamente primos com n. Então,*

$$a_1 a_2 \dots a_{\phi(n)} \equiv -1 \,(\mathrm{mod}\, n).$$

Prova. Como n possui raiz primitiva, temos que $n = 2$, 4, p^k ou $2p^k$.

Se $n = 2$, não há nada a fazer. Se $n = 4$, temos que $\phi(4) = 2$, $a_1 = 1$, $a_2 = 3$ e $1 \cdot 3 = 3 \equiv -1 \pmod 4$.

Suponha que $n = p^k$ ou $n = 2p^k$, em que p é um primo ímpar, e seja a uma raiz primitiva módulo n. Sabemos que o conjunto $R = \left\{a, a^2, \ldots, a^{\phi(n)}\right\}$ é um sistema reduzido de resíduos módulo n, logo, cada elemento de R é congruente a um único elemento do conjunto $\{a_1, a_2, \ldots, a_{\phi(n)}\}$. Assim,

$$\begin{aligned} a_1 a_2 \ldots a_{\phi(n)} &\equiv a \cdot a^2 \cdots a^{\phi(n)} \pmod n \\ &\equiv a^{1+2+\ldots+\phi(n)} \pmod n \\ &\equiv a^{\frac{\phi(n)(\phi(n)+1)}{2}} \pmod n. \end{aligned}$$

Como vimos no final da demonstração do teorema anterior, $\phi(n)$ é par se $n > 2$, logo,

$$\begin{aligned} a_1 a_2 \ldots a_{\phi(n)} &\equiv a^{\frac{\phi(n)^2+\phi(n)}{2}} \pmod n \\ &\equiv a^{\frac{\phi(n)^2}{2}} \cdot a^{\frac{\phi(n)}{2}} \pmod n \\ &\equiv \left(a^{\phi(n)}\right)^{\frac{\phi(n)}{2}} \cdot a^{\frac{\phi(n)}{2}} \pmod n. \end{aligned}$$

Mas, pelo Teorema de Euler, temos que $a^{\phi(n)} \equiv 1 \pmod n$; desse modo,

$$a_1 a_2 \ldots a_{\phi(n)} \equiv a^{\frac{\phi(n)}{2}} \pmod n.$$

Também pelo teorema de Euler,

$$n \mid (a^{\phi(n)-1}) = \left(a^{\frac{\phi(n)}{2}} + 1\right)\left(a^{\frac{\phi(n)}{2}} - 1\right).$$

Mas p é primo ímpar e $p \mid p^k \mid n$, logo, somente um dos fatores $a^{\frac{\phi(n)}{2}} + 1$ ou $a^{\frac{\phi(n)}{2}} - 1$ é divisível por p (e também por p^k).

Como observamos na demonstração do teorema 7, podemos escolher a ímpar. Logo, $a^{\frac{\phi(n)}{2}} + 1$ e $a^{\frac{\phi(n)}{2}} - 1$ são

ambos pares. Daí, sendo $n = p^k$ ou $n = 2p^k$, temos que $n \mid \left(a^{\frac{\phi(n)}{2}} + 1\right)$ ou $n \mid \left(a^{\frac{\phi(n)}{2}} - 1\right)$. Mas $n \nmid \left(a^{\frac{\phi(n)}{2}} - 1\right)$, pois o contrário acarretaria

$$a^{\frac{\phi(n)}{2}} \equiv 1 \,(\mathrm{mod}\, n),$$

o que não pode acontecer, uma vez que $\frac{\phi(n)}{2} < \phi(n) = \mathrm{ord}_n(a)$. Logo, $n \mid \left(a^{\frac{\phi(n)}{2}} + 1\right)$ e

$$a_1 a_2 \ldots a_{\phi(n)} \equiv a^{\frac{\phi(n)}{2}} \equiv -1 \,(\mathrm{mod}\, n).$$

□

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 resultados da aula passada que serão utilizados para demonstrar os resultados desta aula. Também é interessante relembrar o Teorema de Wilson e perguntar aos alunos por que o teorema 9 é uma generalização desse resultado.

A seção 7.2 da referência [1] traz várias outras aplicações não triviais da existência de raízes primitivas módulo n, quando $n = 2$, 4, p^k ou $2p^k$, com p primo ímpar e $k \geq 1$ inteiro.

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.