Ordem e Raízes Primitivas

Nicholas Farrel

1 Definições Básicas: Ordem

Definição: Tome n $>$ 1 e a inteiros tais que $mdc(a, n) = 1$, o menor inteiro positivo k tal que tal que $a^k \equiv 1 \pmod{n}$ (ou $n/a^k - 1$) é chamado de a ordem de a módulo n. A partir deste momento, usaremos a notação $ord_n a$ para representar a ordem de a módulo n.
Observação: Como do Teorema de Euler temos que $a^{\varphi(n)} \equiv 1 \pmod{n}$, sabemos que $1 \leq ord_n a \leq \varphi(n)$.

Os três teoremas a seguir e seus corolários serão as bases para os nossos estudos de Ordem e Raízes Primitivas:

2 Teoremas Iniciais

Teorema 1. Sejam $a, n \in \mathbb{Z}$, com $n > 1$ tais que $mdc(a, n) = 1$ e $k = ord_n a$. Então, $a^h \equiv 1 \pmod{n} \iff k/h$.
Prova da Volta. Como $k = ord_n a \Rightarrow a^k \equiv 1 \pmod{n}$. Como $k/h \Rightarrow h = k \cdot h_0$, $h_0 \in \mathbb{Z}_{>0}$. Então, temos que:

$$a^h = a^{k \cdot h_0} = (a^k)^{h_0} \equiv 1^{h_0} = 1 \pmod{n} \Rightarrow a^h \equiv 1 \pmod{n} \blacksquare$$

Prova da Ida. Assuma que $a^h \equiv 1 \pmod{n}$. Aplicando o algorítimo da divisão em h e k, tome $h = k \cdot q + r$, com $q, r \in \mathbb{Z}_{\geq 0}$ e $0 \leq r \leq k - 1$, assim, como $a^h \equiv 1 \pmod{n} \Rightarrow$

$$1 \equiv a^h = a^{k \cdot q + r} = (a^k)^q \cdot a^r \equiv 1^q \cdot a^r = a^r \pmod{n} \Rightarrow a^r \equiv 1 \pmod{n}$$

Se $r \neq 0$, temos um absurdo, já que $r < k$, e k é a ordem de a módulo n. (O absurdo vem da própria definição dada de ordem.). Logo, $r = 0 \Rightarrow k/h \blacksquare$

Corolário: Em particular, como $a^{\varphi(n)} \equiv 1 \pmod{n}$ (Teorema de Euler), temos que $ord_n a/\varphi(n)$.

Teorema 2. Sejam $a, n \in \mathbb{Z}$, com $n > 1$ tais que $mdc(a, n) = 1$ e $k = ord_n a$. Temos que para todos $i, j \in \mathbb{Z}_{>0}$, $a^i \equiv a^j \pmod{n} \iff i \equiv j \pmod{ord_n a}$.
Prova da Ida. Suponha sem perda de generalidade que $i \geq j$ e que $a^i \equiv a^j \pmod{n}$. Como $mdc(a, n) = 1 \Rightarrow mdc(a^j, n) = 1 \Rightarrow$ dividindo a última congruência por a^j temos: $a^{i-j} \equiv 1 \pmod{n} \Rightarrow$ do *Teorema 1*, $ord_n a/i - j \Rightarrow i \equiv j \pmod{ord_n a} \blacksquare$
Prova da Volta. Suponha que $i \equiv j \pmod{ord_n a} \Rightarrow k/i - j \Rightarrow i - j = k \cdot q, q \in \mathbb{Z}_{\geq 0}$. Disso, temos que $i = j + k \cdot q \Rightarrow$

$$a^i = a^{j+k \cdot q} = (a^k)^q \cdot a^j \equiv 1^q \cdot a^j = a^j \pmod{n} \Rightarrow a^i \equiv a^j \pmod{n} \blacksquare$$

Corolário: As potências $a^1, a^2, \ldots, a^{ord_n a}$ são duas a duas incongruentes no módulo n.
Prova. Se existem dois indices $i, j \in \{1, 2, \ldots, ord_n a\}$ com $i > j$ e $a^i \equiv a^j \pmod{n}$, temos que, do *Teorema 2* $k/i - j$, porém $i \leq i - j \leq k - 1$, o que gera absurdo. Logo, tais índices não existem$\blacksquare$

Teorema 3. Sejam $a, n \in \mathbb{Z}$, com $n > 1$ tais que $mdc(a, n) = 1$ e $k = ord_n a$. Temos que :

$$ord_n a^h = \frac{k}{mdc(h, k)}, \forall h \in \mathbb{Z}_{>0}$$

Prova. Tome $l = ord_n a^h$ e seja $d = mdc(h, k) \Rightarrow h = d \cdot h_0, k = d \cdot k_0$ com $h_0, k_0 \in \mathbb{Z}_{>0}; mdc(h_0, k_0) = 1$.
Sabemos que $a^k \equiv 1 \pmod{n}$ e $(a^h)^l \equiv 1 \pmod{n} \Rightarrow a^{h \cdot l} \equiv 1 \pmod{n} \Rightarrow k/h \cdot l$ (do Teorema 1) $\Rightarrow d \cdot k_0/d \cdot h_0 \cdot l \Rightarrow k_0/h_0 \cdot l$, assim, como $mdc(k_0, h_0) = 1 \Rightarrow k_0/l \Rightarrow l \geq k_0$ ***(1)***.
Por outro lado, $(a^h)^{k_0} = a^{h \cdot k_0} = a^{d \cdot h_0 \cdot k_0} = (a^{d \cdot k_0})^{h_0} = (a^k)^{h_0} \equiv 1^{h_0} = 1 \pmod{n} \Rightarrow$
$(a^h)^{k_0} \equiv 1 \pmod{n}$, logo, como l é a ordem de a^h módulo $n \Rightarrow l \leq k_0$ ***(2)***.
De *(1)* e *(2)* temos que $l = k_0 \Rightarrow k = d \cdot l \Rightarrow l = \frac{k}{d} \Rightarrow ord_n a^h = \frac{k}{mdc(k,h)} \blacksquare$
Corolário: Se $k = ord_n a$, então $ord_n a^h = k \iff mdc(k, h) = 1$.

Agora, encorajo o leitor a tentar resolver os seguintes exemplos antes de ler suas respectivas soluções:

Exemplo 1. Prove que $n/\varphi(a^n-1)$ para todos os inteiros positivos a, n.

(Olimpíada de Matemática de São Petesburgo)

Solução. Veja que, $mdc(a, a^n-1) = 1$, além disso, é fácil ver que $ord_{a^n-1}a = n$, logo, do Corolário do *Teorema 1* temos que: $n/\varphi(a^n-1)$■

Exemplo 2. Encontre o menor inteiro positivo n com a seguinte propriedade:

$$2^{2005}/17^n - 1$$

Solução. Em outras palavras, como $mdc(2^{2005}, 17) = 1$, temos que $n = ord_{2^{2005}}17$. Sabemos pelo Corolário do *Teorema 1* que $n/\varphi(2^{2005}) \Rightarrow n/2^{2004}$, logo $n = 2^k$, onde $k \in \{1, 2, \ldots, 2004\} \Rightarrow 2^{2005}/17^{2^k} - 1$, agora basta acharmos o menor k para o qual esta relação é válida. Usando a fatoração $a^2 - b^2 = (a-b)\cdot(a+b)$:

$$17^{2^k} - 1 = (17^{2^{k-1}} - 1)\cdot(17^{2^{k-1}} + 1) = (17^{2^{k-2}} - 1)\cdot(17^{2^{k-2}} + 1)\cdot(17^{2^{k-1}} + 1) = \ldots$$
$$= (17-1)\cdot(17+1)\cdot(17^2+1)\ldots(17^{2^{k-1}}+1)$$

Vamos então descobrir o expoente de 2 na fatoração de $17^{2^k} - 1$. Veja que, $\forall i \in \mathbb{Z}_{\geq 0}$ temos: $2/17^{2^i} + 1$ e $17^{2^i} + 1 \equiv (-1)^{2^i} + 1 \equiv 1 + 1 = 2 \pmod 4 \Rightarrow 17^{2^i} + 1$ é múltiplo de 2 e não de 4, logo, cada fator $17^{2^i} + 1$ de $17^{2^k} - 1$ contribui com uma unidade para $v_2(17^{2^k} - 1) \Rightarrow v_2(17^{2^k} - 1) = 4+1+1+\cdots+1 = k+4$, logo, como $2^{2005}/17^{2^k} - 1 \Rightarrow k+4 \geq 2005 \Rightarrow k \geq 2001$, assim, como k é mínimo, temos que $k = 2001 \Rightarrow n = 2^{2001}$ é o menor inteiro positivo que satisfaz o problema ■

3 Raízes Primitivas

Definição: Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $mdc(a, n) = 1$. Quando ocorrer de $ord_n a = \varphi(n)$, diremos que a é uma raiz primitiva módulo n.

Teorema 4. Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $mdc(a, n) = 1$. Considere $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$ os inteiros menores ou iguais a n primos com n. Assim, a é uma raiz primitiva módulo n se e somente se:

$$\{a^1, a^2, \ldots, a^{\varphi(n)}\} \equiv \{a_1, a_2, \ldots, a_{\varphi(n)}\} \pmod{n}$$

Prova da Ida. Assuma que a é raiz primitiva módulo $n \Rightarrow ord_n a = \varphi(n)$. Pelo Corolário do *Teorema 2* sabemos que $a^1, a^2, \ldots, a^{\varphi(n)}$ são dois a dois incongruentes no módulo n. Como $mdc(a, n) = 1 \Rightarrow mdc(a^i, n) = 1$,$\forall i \in \mathbb{Z}_{\geq \mathbb{0}} \Rightarrow$ no conjunto $\{a^1, a^2, \ldots, a^{\varphi(n)}\}$ temos $\varphi(n)$ números incongruentes dois a dois no módulo n e primos com $n \Rightarrow$

$$\{a^1, a^2, \ldots, a^{\varphi(n)}\} \equiv \{a_1, a_2, \ldots, a_{\varphi(n)}\} \pmod{n} \blacksquare$$

Prova da Volta. Se $\{a^1, a^2, \ldots, a^{\varphi(n)}\} \equiv \{a_1, a_2, \ldots, a_{\varphi(n)}\} \pmod{n} \Rightarrow a^1, a^2, \ldots, a^{\varphi(n)}$ são incongruentes dois a dois no módulo n, logo, pode haver apenas um congruente a 1 no módulo n, este sendo $a^{\varphi(n)}$, pelo Teorema de Euler, logo, $ord_n a = \varphi(n) \Rightarrow a$ é raiz primitiva módulo $n \blacksquare$

Teorema 5. Se um inteiro positivo n possuir uma raiz primitiva módulo n, então ele terá ao todo exatamente $\varphi(\varphi(n))$ raízes primitivas no módulo n.

Prova. Seja a uma raiz primitiva módulo n. Sabemos do *Teorema 4* que $\{a^1, a^2, \ldots, a^{\varphi(n)}\} \equiv \{a_1, a_2, \ldots, a_{\varphi(n)}\} \pmod{n}$. Tome então g uma raiz primitiva qualquer no módulo n, assim $mdc(g, n) = 1 \Rightarrow$

$$\begin{cases} g \equiv a^i, \text{ para alugm } i \in \{1, 2, \ldots, \varphi(n)\} \\ g \equiv a_j, \text{ para algum } j \in \{1, 2, \ldots, \varphi(n)\} \end{cases}$$

Assim, $ord_n a^i = ord_n g = \varphi(n) \Rightarrow$ (do *Teorema 3*) $\varphi(n) = \frac{ord_n a}{mdc(i, ord_n a)} = \frac{\varphi(n)}{mdc(i, \varphi(n))} \Rightarrow mdc(i, \varphi(n)) = 1$. Logo, o número de raízes primitivas módulo n é igual ao número de $i's \in \{1, 2, \ldots, \varphi(n)\}$ tais que $mdc(i, \varphi(n)) = 1 \Rightarrow$ sabemos que este número é $\varphi(\varphi(n))$ pela definição da função $\varphi \blacksquare$

Vamos resolver alguns exemplos de aplicações destes Teoremas:

Exemplo 3. Se g é uma raiz primitiva de um primo ímpar p, prove que:

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Solução. Vejamos: $0 \equiv g^{p-1} - 1 = (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) \pmod{p} \Rightarrow p/g^{\frac{p-1}{2}} - 1$ ou $p/g^{\frac{p-1}{2}} + 1$.
Sabemos que, como $ord_p g = p-1 > \frac{p-1}{2} \Rightarrow p \nmid g^{\frac{p-1}{2}} - 1 \Rightarrow p/g^{\frac{p-1}{2}} + 1 \Rightarrow g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$■

Exemplo 4. Seja p um primo ímpar. Prove que:

$$1^i + 2^i + \cdots + (p-1)^i \equiv 0 \pmod{p}, \forall i \in \{1, 2 \ldots, p-2\}$$

Solução. Defina $S_i = 1^i + 2^i + \cdots + (p-1)^i$, para todo i de 1 a $p-2$. Tome então para r uma raiz primitiva de p (mostraremos que esta raiz primitiva existe mais futuramente no material). Pelo *Teorema 4* sabemos que:

$$\{r^1, r^2, \ldots, r^{p-1}\} \equiv \{1, 2, \ldots, p-1\} \pmod{p}$$

Então, temos que:

$$S_i \equiv (r^1)^i + (r^2)^i + \cdots + (r^{p-1})^i = r^i + (r^i)^2 + \cdots + (r^i)^{p-1} = \frac{r^i((r^i)^{p-1} - 1)}{r^i - 1} = \frac{r^{ip} - r^i}{r^i - 1} \pmod{p} \Rightarrow$$

$$S_i \equiv \frac{r^{ip} - r^i}{r^i - 1} \pmod{p}$$

Como $ord_p r = \varphi(p) = p - 1$ e $i \leq p-2 \Rightarrow r^i \not\equiv 1 \pmod{p} \Rightarrow p \nmid r^i - 1 \Rightarrow$

$$S_i(r^i - 1) \equiv (r^p)^i - r^i \equiv r^i - r^i \equiv 0 \pmod{p} \Rightarrow p/S_i(r^i - 1) \Rightarrow p/S_i, \forall\ 1 \leq i \leq p-2$$■

Exemplo 5. Seja $p > 2$ um primo e seja a uma raiz primitiva de p. Prove que $(-a)$ é uma raiz primitiva módulo p se e somente se $p \equiv 1 \pmod{4}$.
Solução. *Ida)* Assuma que $(-a)$ também é raiz primitiva módulo p, daí:

$$\begin{cases} ord_p a = p-1 \Rightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \\ ord_p(-a) = p-1 \Rightarrow (-a)^{\frac{p-1}{2}} \equiv -1 \pmod{p} \end{cases} \Rightarrow -1 \equiv a^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \equiv (-1) \cdot (-1)^{\frac{p-1}{2}} \pmod{p} \Rightarrow$$

$\Rightarrow (-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Rightarrow 2/\frac{p-1}{2} \Rightarrow 4/p-1 \Rightarrow p \equiv 1 \pmod{4}$.
Volta) Assuma que $p \equiv 1 \pmod{4}$. Seja $d = ord_p(-a) \Rightarrow (-a)^d \equiv 1 \pmod{p} \Rightarrow a^{2d} \equiv 1 \pmod{p} \Rightarrow$ como a é raiz primitiva de $p \Rightarrow p - 1/2d \Rightarrow \frac{p-1}{2}/d$ *(1).*
Como $p \equiv 1 \pmod{4} \Rightarrow \frac{p-1}{2}$ é par, assim:$a^{\frac{p-1}{2}} = (-a)^{\frac{p-1}{2}} \Rightarrow (-a)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ *(2).*
Sabemos que $1 \leq d \leq p-1 \Rightarrow$ de (1), $d = \frac{p-1}{2}$ ou $p-1$, porém, de (2) $d \neq \frac{p-1}{2} \Rightarrow d = p - 1 = \varphi(p) \Rightarrow (-a)$ é raiz primitiva módulo p■

4 Quais os inteiros que possuem Raízes Primitivas?

Vamos enunciar e provar alguns lemas e teoremas que nos ajudarão a responder esta pergunta:

Teorema de Lagrange: Considere um polinômio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ de coeficientes inteiros ($n \in \mathbb{Z}_{>0}$) e p um primo tal que $p \nmid a_n$. Assim, a congruência $f(x) \equiv 0 \pmod{p}$ tem no máximo n soluções incongruentes módulo p.
Prova. Vamos provar por indução no grau n do polinômio.
Caso Inicial: $n = 1 \Rightarrow f(x) = a_1 x + a_0; p \nmid a_1$, daí, $f(x) \equiv 0 \pmod{p} \iff a_1 x \equiv -a_0 \pmod{p}$ e como $mdc(a_1, p) = 1$, pela teoria das congruências lineares, temos no máximo uma solução no módulo p.
Hipótese: Assuma que, para $k \geq 1$ inteiro se $f(x) = a_k x^k + \cdots + a_1 x + a_0$ é um polinômio de coeficientes inteiros com $p \nmid a_k$, então a congruência $f(x) \equiv 0 \pmod{p}$ tem no máximo k soluções incongruentes módulo p.
Passo Indutivo: Temos que provar que tal fato é válido para um polinômio de grau $k+1$. Seja $P(x)$ um polinomio de coeficientes inteiros e grau $k+1$, se $P(x) \equiv 0 \pmod{p}$ não possui soluções, claramente temos menos de $k+1$ soluções.
Suponha que a congruência $P(x) \equiv 0 \pmod{p}$ tem ao menos uma solução $a \Rightarrow P(a) \equiv 0 \pmod{p} \Rightarrow$ pelo algorítimo da divisão entre polinômios, podemos escrever:

$$P(x) = (x - a) \cdot q(x) + r, \text{ onde } q(x) \in \mathbb{Z}_{[x]}, r \in \mathbb{Z} \tag{1}$$

como $P(a) \equiv 0 \pmod{p} \Rightarrow r \equiv 0 \pmod{p} \Rightarrow p/r$. Além disso, $deg(P) = k+1 \Rightarrow deg(q) = k$
Seja b qualquer outra solução a congruência $P(x) \equiv 0 \pmod{p}$ (se b não existe, a congruência tem 1 raiz, ou seja, menos que $k+1$). Assim,$P(b) \equiv 0 \pmod{p}$ e $a \not\equiv b \pmod{p}$. Substituindo b em (1) $\Rightarrow (b-a) \cdot q(b) + r \equiv 0 \pmod{p} \Rightarrow (b-a) \cdot q(b) \equiv 0 \pmod{p} \Rightarrow$ como $a \not\equiv b \pmod{p} \Rightarrow b - a \not\equiv 0 \Rightarrow q(b) \equiv 0 \pmod{p} \Rightarrow$ por hipótese, como o grau de q é k, há no máximo k soluções incongruentes módulo p para a congruência $q(x) \equiv 0 \pmod{p}$.
Portanto, $P(x) \equiv 0 \pmod{p}$ tem como soluções a adicionado de todas as souluções de $q(x)$, nos dando que $P(x) \equiv 0 \pmod{p}$ possui no máximo $k+1$ soluções, e o resultado segue por indução ■

Corolário: Seja p um primo tal que $d/p-1$. Então, a congruência $x^d - 1 \equiv 0 \pmod{p}$ tem exatamente d soluções incongruentes módulo p.
Prova. Seja $p - 1 = d \cdot c$. Pelo Pequeno Teorema de Fermat, sabemos que a congruência $x^{p-1} - 1 \equiv 0 \pmod{p}$ tem exatamente $p-1$ soluções módulo p, estas sendo os números de 1 a $p-1 \Rightarrow$

$$0 \equiv x^{p-1} - 1 = x^{d \cdot c} - 1 = (x^d)^c - 1 = (x^d - 1)(1 + x^d + x^{2d} + \cdots + x^{(c-1)d}) \pmod{p}$$

Pelo Teorema de Lagrange, $x^d - 1$ e $1 + x^d + x^{2d} + \cdots + x^{(c-1)d}$ possuem respectivamente no máximo d e $dc - d$ raízes módulo p, porém, como cada uma dessas também é raiz de $x^{p-1} - 1$ e $dc - d + d = dc = p - 1$, devemos ter cada polinômio com sua quantidade máxima de raízes, assim finalizando que $x^d - 1$ tem exatamente d raízes módulo p■

Lema 1. Para $n \geq 3,\ 2^n$ não possui raiz primitiva.
Prova. Vamos provar por indução em n que se a é um inteiro impar $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ para todo inteiro $n \geq 3$
Caso Inicial: n = 3, assim, basta observarmos se as congruencias ímpares módulo 8 são satisfeitas.

$$1^2 \equiv 1 \pmod 8$$
$$3^2 \equiv 1 \pmod 8$$
$$5^2 \equiv 1 \pmod 8$$
$$7^2 \equiv 1 \pmod 8$$

Hipótese de Indução: Tome um inteiro $k \geq 3$ tal que se a é um inteiro ímpar $a^{2^{k-2}} \equiv 1 \pmod{2^k}$.
Passo Indutivo:

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} \Rightarrow 2^k / a^{2^{k-2}} - 1 \Rightarrow a^{2^{k-2}} - 1 = 2^k \cdot l \Rightarrow a^{2^{k-2}} = 2^k \cdot l + 1, l \in \mathbb{Z}_{>\mathbb{0}} \Rightarrow$$

$$(\mathrm{a}^{2^{k-2}})^2 = (2^k \cdot l + 1)^2 \Rightarrow a^{2^{k-1}} = 2^{2k} \cdot l^2 + 2^{k+1} \cdot l + 1 \Rightarrow a^{2^{k-1}} = 2^{k+1}(2^{k-1} \cdot l^2 + l) + 1$$

Assim, temos que $a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}\square$
Agora, veja que se existe raiz primitiva a no módulo 2^n para $n \geq 3 \Rightarrow a$ é ímpar, logo, da indução $a^{2^{n-2}} \equiv 1 \pmod{2^n}$. Por outro lado, a é raiz primitiva $\Rightarrow \varphi(2^n)/2^{n-2} \Rightarrow 2^{n-1}/2^{n-2}$ o que é um absurdo, concluindo então que para $n \geq 3,\ 2^n$ não possui raiz primitiva ■

Lema 2. Se p é um primo, p possui raiz primitiva.
Prova. Se $p = 2 \Rightarrow \varphi(2) = 1 \Rightarrow$ como $1^1 \equiv 1 \pmod 2 \Rightarrow 1$ é raiz primitiva módulo 2.
Seja então p um primo ímpar e d um divisor de $p - 1$. Defina a função $F(d)$ para ser o número de inteiros positivos i menores que p tais que $ord_p i = d$. Observe que para todo $i \in \{1, 2, \ldots, p-1\}$, pelo Pequeno Teorema de Fermat, $i^{p-1} \equiv 1 \pmod p \Rightarrow ord_p i / p - 1 \Rightarrow$ todos os inteiros positivos menores que p tem ordem que divide $p - 1 \Rightarrow$

$$p - 1 = \sum_{d/p-1} F(d) \tag{1}$$

porém, das propriedades da função φ, sabemos que:

$$p - 1 = \sum_{d/p-1} \varphi(d) \tag{2}$$

Considere a congruência $x^d \equiv 1 \pmod p$ onde d é um divisor de $p - 1$, pelo Corolário do Teorema de Lagrange, sabemos que este polinômio tem exatamente d raízes no módulo p. Suponha que há ao menos um inteiro a, tal que $ord_p a = d \Rightarrow a$ é raiz de $x^d \equiv 1 \pmod p$, assim já que $(a^i)^d = (a^d)^i \equiv 1^i \equiv 1 \pmod p \forall i \in \mathbb{Z}_{>}\mathbb{0}$, e, pelo Corolário do *Teorema 2*, $\{a^1, a^2, \ldots, a^d\}$ são potências duas a duas incongruentes módulo $p \Rightarrow \{a^1, a^2, \ldots, a^d\}$ são raízes da congruência. Vamos ver quais delas tem ordem d no módulo p.

Pelo *Teorema 3* temos que: $ord_p a^i = \frac{d}{mdc(i,d)} \Rightarrow ord_p a^i \cdot mdc(i,d) = d \Rightarrow ord_p a^i = d \iff mdc(i,d) = 1$, daí, como temos $\varphi(d)$ números de 1 a d que são primos com d, temos então $\varphi(d)$ números menores que p com ordem igual a $d \Rightarrow$.

$$F(d) = \varphi(d) \text{ ou } 0 \tag{3}$$

De (1), (2) e (3), chegamos à conclusão de que $F(d) = \varphi(d)$ para todo divisor d de $p-1 \Rightarrow F(p-1) = \varphi(p-1) \geq 1$, assim, há ao menos um inteiro de 1 a $p-1$ com ordem $p-1$ módulo $p \Rightarrow$ todo primo ímpar p possui raíz primitiva!■

Lema 3. Se p é um primo impar com raiz primitiva r, então, r ou $r+p$ é raiz primitiva módulo p^2.
Prova. Sabemos que $ord_p r = \varphi(p) = p-1$. Tome então $ord_{p^2} r = m$, assim $r^m \equiv 1 \pmod{p^2} \Rightarrow r^m \equiv 1 \pmod{p} \Rightarrow$ pelo *Teorema 1* $p-1/m$. Pelo mesmo teorema, como $m = ord_{p^2} r \Rightarrow m/\varphi(p^2) \Rightarrow m/p(p-1)$ assim, como $mdc(p, p-1) = 1$, m divide ou p ou $p-1$ e como $p-1/m \Rightarrow m = p-1$ ou $p(p-1)$.
*i)*Se $m = p(p-1) \Rightarrow ord_{p^2} r = \varphi(p^2) \Rightarrow r$ é raiz primitiva módulo p^2.
*ii)*Se $m = p-1 \Rightarrow r^{p-1} \equiv 1 \pmod{p^2}$. Seja $s = r+p$, assim, s também é raiz primitiva módulo $p \Rightarrow$ Pelo desenvolvimento inicial, $ord_{p^2} s = p-1$ ou $p(p-1)$. Porém:

$s^{p-1} = (r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + \cdots + p^{p-1} \equiv r^{p-1} + (p-1)pr^{p-2} \equiv 1 + p^2 r^{p-2} - pr^{p-2} \pmod{p^2} \Rightarrow$
$s^{p-1} \equiv 1 - pr^{p-2} \pmod{p^2} \Rightarrow p^2/s^{p-1} - 1 + pr^{p-2}$.

Se $s^{p-1} \equiv 1 \pmod{p^2} \Rightarrow p^2/s^{p-1} - 1 \Rightarrow p^2/pr^{p-2} \Rightarrow p/r^{p-2}$ o que é um absurdo já que r é raiz primitiva módulo p e $mdc(p,r) = 1$. Logo, temos que $s^{p-1} \not\equiv 1 \pmod{p^2} \Rightarrow ord_{p^2} s = p(p-1) = \varphi(p^2) \Rightarrow s$ é raiz primitiva módulo p^2■

Lema 4. Seja p um primo ímpar. Então, qualquer potência p^m possui raiz primitiva. Além disso, se r é uma raiz primitiva módulo p^2, então r é raiz primitva módulo p^m para todos os inteiros positivos m.
Prova. Pelo *Lema 3* sabemos que todo primo p tem uma raiz primitiva r que também é raiz primitiva módulo $p^2 \Rightarrow p^2 \nmid r^{p-1} - 1$. Vamos provar por indução que:

$$p^m \nmid r^{p^{m-2}(p-1)} - 1; \forall \text{ inteiro } m \geq 2.$$

Como o caso inicial $m = 2$ e a hipótese já foram apresentados, vamos para o passo indutivo:
Passo Indutivo: Seja m um inteiro maior que um que satisfaça a hipótese. Como $mdc(r,p) = 1 \Rightarrow mdc(r, p^{m-1}) = 1$. Assim, pelo Teorema de Euler:

$$p^{m-1}/r^{\varphi(p^{m-1})} - 1 \Rightarrow p^{m-1}/r^{p^{m-2}(p-1)} - 1$$

então, existe inteiro k tal que $r^{p^{m-2}(p-1)} = 1 + kp^{m-1}$, onde $p \nmid k$, caso contrário, $r^{p^{m-2}(p-1)} \equiv 1 \pmod{p^m}$, o que é absurdo pela hipótese. Temos então:

$$(r^{p^{m-2}(p-1)})^p = (1+kp^{m-1})^p = \sum_{i=0}^{p} \binom{p}{i} (kp^{m-1})^i \equiv 1 + kp^m \pmod{p^{m+1}} \Rightarrow$$
$$r^{p^{m-1}(p-1)} - 1 \equiv kp^m \pmod{p^{m+1}}$$

e como $p \nmid k \Rightarrow kp^m \not\equiv 0 \pmod{p^{m+1}} \Rightarrow p^{m+1} \nmid r^{p^{m-1}(p-1)} - 1$ e o resultado segue por indução □

Agora, vamos utilizar o resultado da indução para demonstrar que p^m possui raiz primitiva $\forall m \in \mathbb{Z}_{>0}$:

Tome $n = ord_{p^m} r$, onde r é raiz primitiva módulo p e p^2. Pelo *Teorema 1* sabemos que $n/\varphi(p^m) \Rightarrow$

$$n/p^{m-1}(p-1) \tag{1}$$

Por outro lado, $r^n \equiv 1 \pmod{p^m} \Rightarrow r^n \equiv 1 \pmod{p} \Rightarrow$ como $ord_p r = \varphi(p) = p-1 \Rightarrow$ do *Teorema 1*:

$$p - 1/n \tag{2}$$

De (1) e (2), temos que $n = p^s(p-1)$, onde $0 \leq s \leq m-1$. Se $s \leq m-2 \Rightarrow r^{p^s(p-1)} \equiv 1 \pmod{p^m} \Rightarrow (r^{p^s(p-1)})^{p^{m-2-s}} \equiv 1 \pmod{p^m} \Rightarrow r^{p^{m-2}(p-1)} \equiv 1 \pmod{p^m}$, o que é um absurdo pela hipótese, logo, $s = m-1 \Rightarrow n = ord_{p^m} r = p^{m-1}(p-1) = \varphi(p^m) \Rightarrow$ r é raiz primitiva módulo p^m■

Lema 5. Considere um primo $p \neq 2$ e seja $s \in \mathbb{Z}_{>0}$, então $2p^s$ tem uma raiz primitiva. Além disso, se r é uma rais primitiva ímpar módulo p^s, então também é uma raiz primitiva módulo $2p^s$, mas se r é par, $r + p^s$ é raiz primitiva módulo $2p^s$.

Prova. Se r é uma raiz primitiva módulo $p^s \Rightarrow ord_{p^s} r = \varphi(p^s) = \varphi(2p^s) \Rightarrow p^s / r^{\varphi(2p^s)} - 1$.

*i)*Se r é ímpar, temos que $2/r^{\varphi(2p^s)} - 1$ e como $mdc(2,p) = 1 \Rightarrow 2p^s / r^{\varphi(2p^s)} - 1$. Se há potência $r^x, x < \varphi(2p^s) = \varphi(p^s)$ que satisfaz, teríamos $r^x \equiv 1 \pmod{p^s}$, o que gera absurdo, já que $ord_{p^s} r = \varphi(p^s)$. Logo, r é raiz primitiva módulo $2p^s$.

*ii)*Se r é par, então $r + p^s$ é ímpar e é raiz primitiva módulo $p^s \Rightarrow ord_{p^s}(r+p^s) = \varphi(p^s) = \varphi(2p^s) \Rightarrow p^s / (r+p^s)^{\varphi(2p^s)} - 1$. E como $2/(r+p^s)^{\varphi(2p^s)} - 1 \Rightarrow 2p^s/(r+p^s)^{\varphi(2p^s)} - 1$, onde $\varphi(2p^s)$ é o menor inteiro que satisfaz, pelo mesmo argumento em *i)*, logo, $r + p^s$ é raiz primitiva módulo $2p^s$■

Lema 6. Se m, n são inteiros positivos maiores que 2, tais que $mdc(m,n) = 1$, então, o número mn não possui raiz primitiva.

Prova. Suponha que g seja uma raiz primitiva de $mn \Rightarrow mdc(g, mn) = 1$ e $ord_{mn} g = \varphi(mn)$ assim, defina:

$$\begin{cases} d = mdc(\varphi(m), \varphi(n)) \\ h = mmc(\varphi(m), \varphi(n)) \end{cases} \Rightarrow dh = \varphi(m) \cdot \varphi(n) = \varphi(mn) \Rightarrow h = \frac{\varphi(mn)}{d} < \varphi(mn)$$

Esta última veio de que $\varphi(x)$ é sempre par para $x > 2 \Rightarrow d \geq 2$. Assim, temos que $h < \varphi(mn) = ord_{mn}g \Rightarrow$

$$g^h \not\equiv 1 \pmod{mn} \tag{1}$$

Além disso, veja que como $d/\varphi(n)$ e $d/\varphi(m)$, pelo Teorema de Euler:

$$\begin{cases} g^h = g^{\frac{\varphi(m)\cdot\varphi(n)}{d}} = (g^{\varphi(n)})^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{n} \\ g^h = g^{\frac{\varphi(m)\cdot\varphi(n)}{d}} = (g^{\varphi(m)})^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{m} \end{cases}$$

Assim, como $mdc(m,n) = 1 \Rightarrow g^h \equiv 1 \pmod{mn} \Rightarrow$ de (1) chegamos a um absurdo, logo, mn não possui raiz primitiva■

Coroláro. Um inteiro positivo que possui 2 fatores primos ímpares não pode ter raiz primitiva (já que tem dois fatores maiores que 2), também, se $n = 2^x \cdot I$, com x, I inteiros maiores que 1 e I ímpar, temos que n não possui raiz primitiva, por ser escrito como produto de dois fatores maiores que dois.

TEOREMÃO. Dos Lemas e Teoremas vistos, o inteiro posivo n tem raiz primitiva se e somente se $n = 2, 4, p^s,$ ou $2p^s$ (onde p é um primo pimpar e s é um inteiro positivo).

5 Problemas

Probelma 1. Mostre que:
a) 2 é raiz primitiva de 3^n.
b) 2 é raiz primitiva de 5^n.
c) 3 é raiz primitiva de 5^n.
d) 10 é raiz primitiva de 7^n.

Problema 2. Sejam $a, n > 2$ inteiros positivos tais que $n/a^{n-1} - 1$ e $n \nmid a^x - 1$, onde $x < n - 1$ e $x/n - 1$. Prove que n é um número primo.

Problema 3. Sejam p, q primos ímpares distintos tais que $p^2/2^q - 1$. Prove que: $2^{p-1} \equiv 1 \pmod{p^2}$.

Problema 4. Encontre todos os primos p, q tais que $pq/2^p + 2^q$.

Problema 5. Prove que para qualquer inteiro $n \geq 2, 3^n - 2^n$ não é divisível por n.

Problema 6. Prove que todos os divisores de $2^{2^n} + 1$ são da forma $k \cdot 2^{n+1} + 1$.

Problema 7. Encontre todos os inteiros positivos a, n tais que:

$$\frac{(a+1)^n - a^n}{n}$$

é um inteiro.

(China TST 2006)

Problema 8. Encontre todos os primos p e q tais que para todo inteiro n, o número $n^{3pq} - n$ é divisível por $3pq$.

(Romania TST 1996)

Problema 9. Mostre que:

$$\frac{x^7 - 1}{x - 1} = y^5 - 1$$

não possui soluções inteiras.

(IMO Shortlist 2006 N5)

Problema 10. Encontre todos os inteiros n tais que n^2 divide $2^n + 1$.

(IMO 1990)

Problema 11. Prove que $n^7 + 7$ nunca é um quadrado perfeito para $n \in \mathbb{Z}_{>0}$.

(USA TST 2008)

6 Bibliografia

Number Theory - Structures, Examples, and Problems
An Introductory Course in Elementary Number Theory - Wissam Raji
Orders Modulo A Prime - Evan Chen