DIVISIBILIDADE, CONGRUÊNCIAS E ARITMÉTICA MÓDULO *n*

Carlos Gustavo Moreira

♦ Nível Avançado

INTRODUÇÃO

Este artigo se propõe a ser uma referência sobre os temas citados no título, que aparecem naturalmente em diversos problemas de Matemática elementar, alguns dos quais serão explicitamente tratados aqui. O estilo é mais conciso do que a maioria dos outros artigos desta revista, o que pode tornar a leitura mais difícil, mas não desanime! Procure entender os enunciados das proposições e os problemas resolvidos e buscar sua propria solução para eles, além de pensar nos problemas propostos e enviar-nos suas soluções. Em caso de qualquer dúvida não deixe de escrever-nos.

Seção 1: Divisão euclidiana e o teorema fundamental da aritmética

Os resultados que seguem têm como base o seguinte fato sobre os inteiros: Dados $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ existem $q, r \in \mathbb{Z}$ com $0 \leq r < b$ e $a = bq + r$. Tais q e r estão unicamente determinados. De fato, $q = [a/b]$ e $r = a - bq$ (aqui [x] denota o único inteiro k tal que $k \leq x < k + 1$). Como conseqüência temos a

Proposição 0 (Divisão Euclidiana): Dados $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$ existem $q, r \in \mathbb{Z}$ unicamente determinados tais que $0 \leq r < |b|$ e $a = bq + r$ ❑

Definição: Dados dois inteiros a e b , com $a \neq 0$ dizemos que a divide b (denotamos $a|b$) se existe c inteiro tal que $b = ac$.

Proposição 1: Dados $a, b \in \mathbb{Z}$ não ambos nulos existe $d \in \mathbb{N}^*$ tal que $d|a$, $d|b$ e, para todo $c \in \mathbb{N}^*$, $c|a$, $c|b \Rightarrow c|d$. Além disso existem $x, y \in \mathbb{Z}$ com $d = ax + by$. (Esse d é chamado o máximo divisor comum entre a e b : $d = mdc\,(a, b)$.)

Demonstração: Seja $A = \{k > 0 \mid \exists\, x, y \in \mathbb{Z}$ tais que $k = ax + by\}$ e seja

$d = ax_0 + by_0$ o menor elemento de A. Mostraremos que $d \mid a$. Como

$d \in \mathbb{N}^*$, existem $q, r \in \mathbb{Z}$ com $a = dq + r$ e $0 \leq r < d$. Queremos mostrar que $r = 0$. De fato, se $r > 0$, $r = a - dq = a(1 - qx_0) + b(-qy_0) \in A$, contradizendo o fato de d ser o menor elemento de A. Portanto, $r = 0$ e

$a = dq \Rightarrow d \mid a$. Do mesmo modo prova-se que $d \mid b$. Suponha agora que $c \mid a$ e $c \mid b$. Então $c \mid ax_0 + by_0 = d$, como queríamos provar ❑

Lema: Se $mdc\,(q, n) = 1$ e $n \mid qk$ então $n \mid k$.

Prova do Lema: Como $mdc(q, n) = 1$, existem $x, y \in \mathbb{Z}$ com $qx + ny = 1$, logo $qkx + nky = k$, portanto $n \mid k$ (pois $\mid qkx$ e $n \mid nky$) ❑

Corolário: Sejam p um número primo e $a, b \in \mathbb{Z}$. Se $p \mid ab$ então $p \mid a$ ou $p \mid b$ ❑

Teorema fundamental da aritmética: Todo número natural $n \geq 2$ possui uma única fatoração (a menos da ordem dos fatores), como produto de primos.

Demonstração: $n = 2$ é primo. Vamos mostrar a existencia da fatoração por primos por indução: Se n é primo não há o que provar. Se n é composto, $n = ab$, $a, b \in \mathbb{N}$, $a < n$, $b < n$ e, por hipótese de indução, a e b se decompõem como produto de primos, portanto n se decompõe como produto de primos.

Vamos agora mostrar a unicidade, também por indução: Suponha que n admita duas fatorações $n = p_1p_2\ldots p_r$ e $n = q_1q_2\ldots q_s$ como produto de primos. O Corolário acima mostra que, como $p_1 \mid q_1q_2\ldots q_r$, p_1 deve dividir algum q_i e portanto $p_1 = q_i$ (pois são ambos números primos) e, como

$n/p_1 = n/q_i < n$ admite uma única fatoração prima, por hipótese de indução, concluímos que a fatoração de n é única ❑

Proposição 2: O conjunto dos números primos é infinito.

Demonstração: Suponha que o conjunto dos números primos seja finito, digamos $\{ p_1, p_2, \ldots, p_n \}$. Nesse caso, o número $N = p_1 p_2 \ldots p_n + 1$ seria maior que todos os primos, mas não divisível por nenhum deles, pois

$p_i \mid (p_1 p_2 \ldots p_n + 1) \Rightarrow p_i \mid 1$, absurdo. Teríamos então um natural $N > 2$ que não seria múltiplo de nenhum primo, contradizendo o teorema fundamental

da aritmética ❑

Obs.: As idéias desta seção podem ser utilizadas em situações mais gerais, como no estudo de polinômios (por exemplo com coeficientes racionais), onde existe um algoritmo de divisão, a partir do qual pode-se provar de modo análogo resultados correspondentes aos aqui apresentados sobre máximo divisor comum, existência e unicidade de fatoração.

Seção 2: Congruências

Definição: Sejam $a, b, n \in \mathbb{Z}$, $n > 0$. Dizemos que a é congruente a b (módulo n) (denota-se $a \equiv b$ (módulo n)) se $n \mid (b - a)$

Obs: $a \equiv a$ (módulo n), $a \equiv b$ (módulo n) $\Leftrightarrow b \equiv a$ (módulo n),

$a \equiv b$ (módulo n), $b \equiv c$ (módulo n) $\Rightarrow a \equiv c$ (módulo n), ou seja, congruência (módulo n) é uma relação de equivalência.

Proposição: Se $a \equiv b$ (módulo n) e $c \equiv d$ (módulo n) então $a + c \equiv b + d$ (módulo n) e $ac \equiv bd$ (módulo n).

Demonstração: $n \mid (b - a)$, $n \mid (d - c) \Rightarrow n \mid (b + d) - (a + c) \Rightarrow (a + c) \equiv$

$(b + d)$ (módulo n), e $bd - ac = b(d - c) + ((b - a) \Rightarrow n \mid (bd - ac) \Rightarrow bd \equiv ac$ (módulo n) ❑

Definição: Dados $n, a \in \mathbb{Z}$ $n > 0$, definimos $\overline{a} = \overline{a}$ (módulo n) =

$= \{k \in \mathbb{Z} \mid k \equiv a$ (módulo $n)\}$.

Dados $a, b \in \mathbb{Z}$ definimos $\overline{a} + \overline{b} = \overline{a+b}$ e $\overline{a} \cdot \overline{b} = \overline{ab}$ (estas operações de soma e produto estão bem definidas pela proposição anterior).

Definimos ainda $\mathbb{Z}/n\mathbb{Z} = \{ \overline{a}$ (módulo n), $a \in \mathbb{Z}\} = \{ \overline{0}, \overline{1}, \overline{2}, \ldots \overline{n-1} \}$. Cada $\overline{a}$ é chamada uma classe de congruência módulo n.

Definição: Sejam $n, a \in \mathbb{Z}$, $n > 0$. Dizemos que a é *invertível* módulo n se existe $b \in \mathbb{Z}$ com $ab \equiv 1$(módulo n) (ou seja, tal que $\overline{a} \cdot \overline{b} = 1$). Dizemos que $\overline{b}$ é o inverso de $\overline{a}$ em $\mathbb{Z}/n\mathbb{Z}$.

Definição: $(\mathbb{Z}/n\mathbb{Z})^* = \{ \overline{a} \mid a \in \mathbb{Z}$ e a é invertível (módulo $n)\}$. Obs. a é *invertível* (módulo n) $\Leftrightarrow$ *mdc (a, n)* $=1$. De fato, *mdc (a, n)* $= 1 \Leftrightarrow \exists\, x, y \in \mathbb{Z}$ tais que $ax + ny = 1 \Leftrightarrow \overline{a} \cdot \overline{x} = \overline{1}$ (módulo n).

Notação: Dado um conjunto finito X, escrevemos $\# X$ para significar o número de elementos de X.

Definição: A função φ de Euler, $\varphi: \mathbb{N} \to \mathbb{N}$ é definida por
$\varphi(n) = \#\,(\mathbb{Z}/n\mathbb{Z})^* = \#\,\{k \in \mathbb{Z} \mid 0 \le k < n$ e *mdc* $(k, n) = 1\}$.

Notemos que se p é um número primo e $k \in \mathbb{N}$ então $\varphi(p^k) = p^k - p^{k-1} =$
$p^k\,(1-1/p)$. De fato, *mdc* $(r, p^k) = 1$ se e só se p não divide r. Logo $\varphi(p^k) = \#\{r \in \mathbb{Z} \mid 0 \le r < p^k$ e *mdc* $(r, p^k) = 1\} = \#\,\{r \in \mathbb{Z} \mid 0 \le r < p^k\} -$
$\#\,\{r \in \mathbb{Z} \mid 0 \le r < p^k$ e $p \mid r\} = p^k - p^{k-1}$.

Definição: n números inteiros $a_1, a_2, \ldots a_n$ formam um sistema completo de resíduos (*s.c.r.*) módulo n se $\{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}\} = \mathbb{Z}/n\mathbb{Z}$ isto é, se os a representam todas as classes de congruência módulo n (por exemplo, $0,1,2,\ldots n-1$ formam um *s.c.r.* (módulo n)).
$\varphi(n)$ números inteiros $b_1, b_2, \ldots b_{\varphi(n)}$ formam um sistema completo de invertíveis (*s.c.i.*) módulo n se $\{\overline{b_1}, \overline{b_2}, \ldots \overline{b_{\varphi(n)}}\} = (\mathbb{Z}/n\mathbb{Z})^*$, isto é, se os b_i representam todas as classes de congruências invertíveis módulo n.

Proposição: Sejam $q, r, n \in \mathbb{Z}$, $n > 0$, q invertível módulo n, $a_1, a_2, \ldots, a_n$ um *s.c.r.* (módulo n) e $b_1, b_2, \ldots, b_{\varphi(n)}$ um *s.c.i.* (módulo n).
Então $qa_1 + r, qa_2 + r, \ldots, qa_n + r$ formam um *s.c.r.* (módulo n) e
$qb_1, qb_2, \ldots qb_{\varphi(n)}$ formam um *s.c.i.* (módulo n).

Demonstração: Vamos provar que se $a_1, \ldots a_n$ formam um *s.c.r.* (módulo n) então $qa_1 + r, \ldots qa_n + r$ formam um *s.c.r.* (módulo n). Basta provar que

$qa_i + r \equiv qa_j + r$ (módulo n) $\Rightarrow i = j$, pois nesse caso teremos n classes de congruências distintas módulo n, que devem ser todas as classes de $\mathbb{Z}/n\mathbb{Z}$.

Seja $y \in \mathbb{Z}$ tal que $qy \equiv 1$ (módulo n).

Temos $qa_i = qa_i + r - r \equiv qa_j + r - r = qa_j$ (módulo n) $\Rightarrow qya_i \equiv qya_j$

(módulo n) $\Rightarrow a_i \equiv a_j$ (*módulo n*) $\Rightarrow i = j$.

Seja agora $b_1, b_2,\ldots b_{\varphi(n)}$ um *s.c.r.* (módulo n). Temos que qb_i é invertível módulo n. para todo i,$1 \leq i \leq \varphi(n)$, pois se x_i é tal que $b_i x_i \equiv 1$ (módulo n). então $(qb_i)\ (x_i y) = (qy)\ (b_i x_i) \equiv 1$ (módulo n). Por outro lado, se $qb_i \equiv qb_j$ (módulo n) então $b_i \equiv yqb_i \equiv yqb_j \equiv b_j$ (módulo n) $\Rightarrow i = j$, e portanto $qb_1,\ qb_2,\ldots qb_{\varphi(n)}$ é um *s.c.i.* (módulo n) ❑

Teorema (Euler): Sejam $a, n \in \mathbb{Z}$, $n > 0$, tais que *mdc* $(a, n) = 1$. Então

$a^{\varphi(n)} \equiv 1$ (módulo n).

Demonstração: Seja $b_1,\ b_2,\ldots b_{\varphi(n)}$ um *s.c.i.* (módulo n) Pela proposição anterior, (ab_1), $(ab_2),\ldots,(ab_{\varphi(n)})$ formam um *s.c.i.* (módulo n), e temos

$\{\ \overline{b}_1,\ \overline{b}_2,\ldots,\ \overline{b}_{\varphi(n)}\} = \{\ \overline{ab}_1,\ \overline{ab}_2,\ldots \overline{ab}_{\varphi(n)}\} = (\mathbb{Z}/n\mathbb{Z})^* \Rightarrow \overline{b}_1 \cdot \overline{b}_2 \ldots\ \overline{b}_{\varphi(n)} = \overline{ab}_1 \cdot \overline{ab}_2 \ldots\ \overline{ab}_{\varphi(n)}$
$= \overline{a}^{\varphi(n)} \cdot \overline{b}_1\ \overline{b}_2\ \ldots\ \overline{b}_{\varphi(n)} \Rightarrow\ \overline{b}_1 \cdot \overline{b}_2 \ldots\ \overline{b}_{\varphi(n)}\ (\ \overline{a}^{\varphi(n)} - \overline{1}) = 0 \Rightarrow\ \overline{a}^{\varphi(n)} = \overline{1}$ pois $b_1,\ b_2,\ldots b_{\varphi(n)}$ são invertíveis (módulo n) $\Rightarrow a^{\varphi(n)} \equiv 1$ (módulo n) ❑

Corolário: (Pequeno Teorema de Fermat): Se $a \in \mathbb{Z}$ e p é primo então

$a^p \equiv a$ (módulo p).

Prova : Se $p \mid a$, então $a^p \equiv a \equiv 0$ (módulo p).

Se p não divide a, então *mdc* $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1$ (módulo p) $\Rightarrow a^p \equiv a$ (módulo p) ❑

Exercício resolvido: Exiba $n \in \mathbb{N}$ tal que 2^n tenha mais de duas mil casas decimais e tenha entre suas 2000 últimas casas decimais 1000 zeros consecutivos.

Solução: $2^{\varphi(5^{2000})} \equiv 1$ (módulo 5^{2000}), pelo teorema de Euler. Portanto,

existe $b \in \mathbb{N}$ com $2^{\varphi(5^{2000})} = 5^{2000}\ b + 1$, e teremos $2^{2000+\varphi(5^{2000})} = 10^{2000}\ b + 2^{2000}$, e portanto os 2000 últimos dígitos de $2^{2000+\varphi(5^{2000})}$ coincidem com a representação decimal de 2^{2000}, que tem no máximo 667 dígitos, pois

$2^3 < 10 \Rightarrow 2^{2000} < 2^{3.667} < 10^{667}$. Desta forma , $2^{2000+\varphi(5^{2000})}$ tem pelo menos 2000 – 667 = 1333 zeros consecutivos dentre as 2000 últimas casas decimais, de modo que $n = 4 \cdot 5^{1999} + 2000$ satisfaz as condições do enunciado (pois $\varphi(5^{2000}) = 4 \cdot 5^{1999}$) ❑

Teorema Chinês dos restos: Se *mdc* $(m, n) = 1$ então
f: $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$,
$f(\ \overline{a}$ (módulo $n)) = (\ \overline{a}$ (módulo m), $\overline{a}$ (módulo n))
é uma bijeção.

Demonstração: f está bem definida, pois se $a = b$ (módulo mn) então $a \equiv b$ (módulo m) e $a \equiv b$ (módulo n). Como $\mathbb{Z}/mn\mathbb{Z}$ e $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ têm mn elementos cada, é suficiente verificar que f é injetiva. E, de fato, se $a \equiv b$ (módulo m) e $a \equiv b$ *(módulo n)* então $m \mid (b - a)$ e $n \mid (b - a) \Rightarrow$
$b - a = mk$, $n \mid mk \Rightarrow n \mid k$, pois *mdc* $(m, n) = 1 \Rightarrow mn \mid (b - a) \Rightarrow a \equiv b$ (módulo mn) ❑

***Corolário*:** Se $m_1, m_{2,\ldots,} m_r \geq 1$ são inteiros, e *mdc* $(m_i, m_j) = 1$ para $i \neq j$ então
f: $\mathbb{Z}/m_1\, m_2,\ldots m_r\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}$,
$f(\ \overline{a}$ (módulo $m_1 \cdot m_2 \ldots . m_r)) = (\ \overline{a}$ (módulo m_1), … , $\overline{a}$ (módulo m_r))
é uma bijeção ❑

Notemos que este Corolário mostra que, dados inteiros $a_1, a_2,\ldots a_r$, existe um inteiro n com $n = a_1$ (módulo m_1), $n \equiv a_2$ (módulo m_2), …, $n \equiv a_r$ (módulo m_r).

Proposição: Temos $f((\mathbb{Z}/mn\mathbb{Z})^*) = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ para a função f definida acima.

Demonstração: Isto segue do fato de que a é primo com mn se e só se a é primo com m e a é primo com n ❑

Corolário: *mdc* $(m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m) \cdot \varphi(n)$ ❑
Como conseqüência, se $n = p_1^{\alpha_1}, p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ *onde* $p_1, p_2,\ldots p_k$ são primos distintos, $\alpha_1, \alpha_2,\ldots \alpha_k \in \mathbb{N}^*$ então $\varphi(n) = n\,(1-1/p_1)\,(1-1/p_2)\ldots(1-1/p_k)$.
Em particular, se $n \geq 3$ então $\varphi(n)$ é par ❑
Vamos mostrar um problema cuja solução usa de modo não trivial o teorema chinês dos restos:

Problema*:* Prove que dado $n \in \mathbb{N}$ existe um conjunto de n elementos $A \subset \mathbb{N}$ tal que para todo $B \subset A$, $B \neq \emptyset$, $\sum_{x \in B} x$ é uma potência não trivial (isto é, um número da forma m^k, onde m, k são inteiros maiores ou iguais a 2), ou seja, $A = \{x_1, x_2,\ldots x_n\}$ tal que $x_1, x_2,\ldots x_n$, $x_1 + x_2$, $x_1 + x_3,\ldots, x_{n-1} + x_n$,
$\ldots, x_1 + x_2 + \ldots x_n$ são todos potências não triviais.

***Solução**: $A = \{4\}$ é solução para $n = 1$, $A = \{9,16\}$ é solução para $n = 2$. Vamos provar a existencia de um tal conjunto por indução em n. Suponha que $A=\{x_1,\ldots, x_n\}$ é um conjunto com n elementos e para todo $B \subset A$, $B \neq \emptyset$, $\sum_{x\in B} x = m_B^{k_B}$ Vamos mostrar que existe $c \in \mathbb{N}$ tal que o conjunto*

$\tilde{A} =\{cx_1, cx_2, \ldots, cx_n, c\}$ satisfaz o enunciado.

Seja $\ell = mmc\ \{k_B, B \subset A, B \neq \emptyset\}$ o mínimo múltiplo comum de todos os exponentes k_B.

Para cada $B \subset A$, $B \neq \emptyset$ associamos um número primo $p_B > \ell$, de forma que $B_1 \neq B_2 \Rightarrow p_{B_1} \neq p_{B_2}$, e associamos um natural r com $r_B \equiv 0$ (módulo p_x), $\forall X \neq B$, $\ell\, r_B + 1 \equiv 0$ (módulo p_B) (tal r_B existe pelo teorema chinês dos restos), e tomamos

$$c = \prod_{\substack{B\subset A\\ B\neq\emptyset}} (1+m_B^{k_B})^{\ell r_B}$$

Como c é uma potência ℓ-ésima, c é uma potência k_B-ésima para todo $B \subset A$, $B \neq \emptyset$, portanto, para $B' \subset \{cx_1, cx_2,\ldots,cx_n\}$, $B' \neq \emptyset$, teremos $B' = \{cx \mid x \in B\}$ para algum $B \subset A$, $B \neq \emptyset$. Logo $\sum_{x\in B'} x$ será uma potência k_B-ésima.

Além disso,

$$\sum_{X\in B'\cup\{c\}} x = c(1+m_B^{K_B}) = \left[\prod_{\substack{X\subset A\\ X\neq\emptyset,B}} (1+m_X^{K_X})^{\ell r_X}\right]\cdot (1+m_B^{K_B})^{\ell r_B+1},$$

que é uma potência p_B-ésima, pois r_X é múltiplo de p_B para $X \neq B$ e $\ell\, r_B + 1$ é múltiplo de p_B ❑

Seção 3: Ordens e raízes primitivas.

Dados $n \in \mathbb{N}^*$ e $a \in \mathbb{Z}$ com $mcd\ (a, n) = 1$, definimos **a ordem de *a* módulo *n***, $ord_n a := min\ \{t \in \mathbb{N}^* \mid a^t \equiv 1(\text{módulo } n)\}$. Dado $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ definidos $ord\ \overline{a} = ord_n a$.

Proposição: $\{t \in \mathbb{N}^* \mid a^t \equiv 1(\text{módulo } n)\} = \{k.ord_n a,\ k \in \mathbb{N}^*\}$.

Demonstração: Como $a^{ord_n a} \equiv 1$ (módulo n), para todo $k \in \mathbb{N}$ tem-se $a^{k.ord_n a} = (a^{ord_n a})^k \equiv 1^k = 1$ (módulo n). Por outro lado, se $t \in n$, $a^t \equiv 1$ (módulo n), existe $k \in \mathbb{N}$ com

$t = k \cdot ord_n a + r, 0 \leq r < ord_n a \Rightarrow a^t = a^{k.ord_n a} \cdot a^r \equiv 1.a^r \equiv a^r$ (módulo n) $\Rightarrow a^r \equiv 1$ (módulo n), portanto $r = 0$ (pois $0 < r < ord_n a$ contradiria a minimalidade de $ord_n a$), e $t = k.\ ord_n a$ ❑

Corolário: $ord_n a \mid \varphi(n)$ ❑

Definição: Se $ord_n a = \varphi(n)$, dizemos que a é **raiz primitiva módulo *n***.

Exemplos: 2 é raiz primitiva módulo 5, pois $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, que é a primeira potência de 2 congruente a 1 módulo 5 e $4 = \varphi(5)$.

• 1 é raiz primitiva módulo 2, pois $ord_2\ 1 = 1 = \varphi(2)$.

• 3 é raiz primitiva módulo 4, pois $\text{ord}_4 3 = 2 = \varphi(4)$.

Proposição 3.1: a é raiz primitiva módulo $n \Leftrightarrow \{ \bar{a}^t, t \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^*$.

Demonstração: Para todo $a \in \mathbb{Z}$ com $mdc\ (a, n) = 1$ temos $\{ \bar{a}^t, t \in \mathbb{N}\} \subset (\mathbb{Z}/n\mathbb{Z})^*$. Se a é raiz primitiva módulo n então os números $1, a, a^2, \ldots a^{\varphi(n)-1}$ são distintos (módulo n) pois $a^i = a^j$ (módulo n), com $0 \le i < j < \varphi(n) \Rightarrow a^{j-i} \equiv 1$ (módulo n) com $0 < j - i < \varphi(n)$, absurdo $\Rightarrow \{a^t, t \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^*$.
Por outro lado, $\#\{ \bar{a}^t, t \in \mathbb{N}\} \le ord_n a$ (o argumento acima mostra que de fato vale a igualdade), e portanto
$\{ \bar{a}^t, t \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^* \Rightarrow ord_n a = \varphi(n)$ ❑

Corolário 1: Se m divide n e a é a raiz primitiva módulo n então a é raiz primitiva módulo m ❑

Corolário 2: Se $k \ge 3$, então não existe nenhuma raiz primitiva módulo 2^k.

Prova: Pelo corolário anterior, basta provar que não existe raiz primitiva módulo 8, e isso segue do fato que se a é ímpar,
$a = 2r + 1, r \in \mathbb{Z} \Rightarrow a^2 = 4r(r + 1) + 1 \equiv 1$ (módulo 8) ❑

Proposição 3.2: Sejam p um número primo, e $a \in \mathbb{Z}$ raiz primitiva módulo p. Então a ou $a + p$ é raiz primitiva módulo p^2.

Demonstração: Por hipótese, $ord_p a = \text{ord}_p(a+ p) = \varphi(p) = p - 1$. Portanto
$p - 1 \mid ord_{p^2} a$ (pois $a^t \equiv 1$ (módulo p^2) $\Rightarrow a^t \equiv 1$(módulo p)), e, como

$ord_{p^2} a \mid \varphi(p^2) = p(p - 1)$, devemos ter $ord_{p^2} a = p - 1$ ou
$ord_{p^2} a = p(p - 1) = \varphi(p^2)$. Do mesmo modo, $ord_{p^2}(a + p) = p - 1$ ou $ord_{p^2}(a + p) = p(p - 1) = \varphi(p^2)$.
Basta provar, portanto, que $ord_{p^2} a \ne p - 1$ ou $ord_{p^2}(a + p) \ne p - 1$.
Suponha que $ord_{p^2} a = p - 1$. Portanto, $a^{p-1} \equiv 1$ (módulo p^2), e então
$(a + p)^{p-1} = a^{p-1} + (p - 1)pa^{p-2} + C_{p-1}^2 a^{p-3} \cdot p^2 + \ldots \equiv 1 + (p - 1)pa^{p-2}$ (módulo p^2), portanto $(a + p)^{p-1}$ não é congruente a 1(módulo p^2), pois p^2 não divide $(p - 1)pa^{p-2}$, donde $ord_{p^2}(a + p) \ne p - 1$ ❑

Proposição 3.3: Se p é um número primo ímpar e a é raiz primitiva módulo p^2 então a é raiz primitiva módulo p^k para todo $k \in \mathbb{N}$.

Demonstração: temos $a^{p-1} \equiv 1$ (módulo p), mas a^{p-1} não é congruente a 1 (módulo p^2), portanto $a^{p-1} = 1 + b_1 p$, onde p não divide b_1. Vamos mostrar por indução que $a^{p^{k-1}(p-1)} = 1 + b_k p^k$, onde p não divide b_k, para todo

$k \geq 1$: Temos $a^{p^k(p-1)} = (a^{p^{k-1}(p-1)})^p = (1 + b_k p^{k-1})^p =$

$= 1 + b_k p^{k+1} + C_p^2 b_k^2 p^{2k} + ... \equiv 1 + b_k p^{k+1}$ (módulo p^{k+2}). Logo

$a^{p^k(p-1)} = 1 + b_k p^{k+1}$, com $b_{k+1} \equiv b_k$ (módulo p). Segue-se que p não divide b_{k+1}.

Vamos agora mostrar por indução que a é raiz primitiva módulo p^k para todo $k \geq 2$. Suponha que a seja raiz primitiva módulo p^k. Então temos

$p^{k-1}(p-1) = \varphi(p^k) = ord_{p^k} a \mid ord_{p^{k+1}} a \mid \varphi(p^{k+1}) = p^k(p-1)$. Portanto,

$ord_{p^{k+1}} a = p^{k-1}(p-1)$ ou $ord_{p^{k+1}} a = p^k(p-1) = \varphi(p^{k+1})$, mas o primeiro caso é impossível, pois $a^{p^{k-1}(p-1)} = 1 + b_k p^k$, que não é congruente a 1 módulo p^{k+1}, pois p não divide b_k. Portanto $ord_{p^{k+1}} a = \varphi(p^{k+1})$ e a é raiz primitiva módulo p^{k+1} ❑

Exemplo: 2 é raiz primitiva módulo 5^k, $\forall k \in \mathbb{N}$. De fato, 2 é raiz primitiva módulo 5, e, como $2^4 = 16 \neq 1$ (módulo 25), 2 é raiz primitiva módulo $25 = 5^2$ (como na proposição 3.2). Portanto, pela proposição 3.3, 2 é raiz primitiva módulo 5^k, $\forall k \in \mathbb{N}$.

Exercício resolvido: Mostre que existe n natural tal que os mil últimos dígitos de 2^n pertencem a $\{1, 2\}$.

Solução: Observamos inicialmente que para todo $k \in \mathbb{N}$ existe um número m_k de k algarismos, todos 1 ou 2, divisível por 2^k.

De fato, $m_1 = 2$ e $m_2 = 12$ satisfazem o enunciado.

Seja $m_k = 2^k \cdot r_k$, $r_k \in \mathbb{N}$. *Se* r_k é par, tome $m_{k+1} = 2 \cdot 10^k + m_k =$

$2^{k+1}(5^k + r_k/2)$, e se r_k é ímpar, tome $m_{k+1} = 10^k + m_k = 2^{k+1}(5^k + r_k)/2$.

Como $m_{1000} \equiv 2$ (módulo 10), 5 não divide $r_{1000} = m_{1000}/2^{1000}$. Como 2 é raiz primitiva módulo 5^{1000}, existe $k \in \mathbb{N}$ *com* $2^k \equiv r_{1000}$ (módulo 5^{1000}). Logo

$2^k = b \cdot 5^{1000} + r_{1000}$, para algum $b \in \mathbb{N}$. Portanto, $2^{k+1000} = b \cdot 10^{1000} +$

$2^{1000} \cdot r_{1000} = b \cdot 10^{1000} + m_{1000}$, e as 1000 últimas casas de 2^{k+1000} são as 1000 casas de m_{1000}, que pertencem todas a $\{1, 2\}$ ❑

Observação: Se p é primo ímpar, $k \in \mathbb{N}$ e a é um inteiro ímpar tal que a é raiz primitiva módulo p^k então a é raiz primitiva módulo $2p^k$, pois $\varphi(p^k) = ord_{p^k} a \mid ord_{2p^k} a \mid \varphi(2p^k) = \varphi(p^k) \Rightarrow ord_{2p^k} a = \varphi(2p^k)$. Isso implica que se a é raiz primitiva módulo p^k então a ou $a + p^k$ é raiz primitiva módulo $2p^k$ (pois a e $a + p^k$ são raízes primitivas módulo p^k e um deles é ímpar.) ❑

Proposição 3.4: Se $n = ab$, com $a \geq 3$ e $b \geq 3$ inteiros tais que $mdc(a, b) = 1$, então não existe raiz primitiva módulo n.

Demonstração: Temos $\varphi(n) = \varphi(a) \cdot \varphi(b)$ e, como $a \geq 3$ e $b \geq 3$, $\varphi(a)$ e $\varphi(b)$ são pares. Se $mdc(k, n) = 1$ então temos $k^{\varphi(n)/2} = (k^{\varphi(b)/2})^{\varphi(a)} \equiv 1$ (módulo a), e $k^{\varphi(n)/2} = (k^{\varphi(a)/2})^{\varphi(b)} \equiv 1$ (módulo b). Assim, $k^{\varphi(n)/2} = 1$(módulo n), e portanto

$ord_n k \mid \varphi(n)/2 < \varphi(n)$ ❑

Teorema: Existe alguma raiz primitiva módulo n se, e só se,
$n = 2$, $n = 4$, $n = p^k$ ou $n = 2p^k$ onde p é primo ímpar.

Prova: Pelos resultados anteriores, basta provar que se p é primo ímpar então existe raiz primitiva módulo p, ou seja, existe $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ com
$\text{ord}_p\, a = p - 1$.
Para cada $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$, tem-se $\text{ord}_p\, a \mid (p-1)$. Seja d um divisor de $p-1$. Definimos $N(d) = \#\{\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^* \mid \text{ord}_p\, a = d\}$.
Temos portanto $p - 1 = \sum_{d \mid p-1} N(d)$. O resultado seguirá dos dois lemas seguintes:

Lema 1: $N(d) \le \varphi(d)$ para todo d divisor de $p-1$.

Prova: Se $N(d) > 0$ então existe $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ com $ord_p\, a$. Se $ord_p\, a = d$, então $\overline{a}^d = \overline{1}$ e, para $0 \le k < d$, as classes de a^k são todas distintas módulo p, e $(\overline{a}^k)^d = \overline{1}$. Como a equação $x^d - \overline{1} = 0$ tem no máximo d raízes distintas em $\mathbb{Z}/p\mathbb{Z}$ (pois $\mathbb{Z}/p\mathbb{Z}$ é um corpo), suas raízes são exatamente $\overline{a}^k$, $0 \le k < d$. Por outro lado, $ord_p\, a^k = d \Rightarrow mcd(k, d) = 1$, pois se $r > 1$ é tal que $r \mid k$ e $r \mid d$ então $(a^k)^{d/r} = (a^d)^{k/r} \equiv 1$(módulo p), logo $\text{ord}_p(a^k) \le d/r < d$. Desta forma, $\{\overline{b} \in (\mathbb{Z}/p\mathbb{Z})^* \mid \text{ord}_p b = d\} \subset \{\overline{a}^k, 0 \le k < d \text{ e } mcd(k,d) = 1\}$, portanto $N(d) \le \varphi(d)$ ❑

Lema 2: $\sum_{d \mid n} \varphi(d) = n$, para todo $n \in \mathbb{N}$.

Prova do Lema 2: Considere os n números racionais $1/n, 2/n, \ldots, n/n$. Ao simplificá-los, aparecem exatamente $\varphi(d)$ deles com denominador d, para cada divisor d de n. Portanto, $\sum_{d \mid n} \varphi(d) = n$ ❑

Fim da prova do teorema:
Do Lema 2 segue que $\sum_{d \mid p-1} \varphi(d) = p - 1$ e, como $p - 1 = \sum_{d \mid p-1} N(d)$ e $N(d) \le \varphi(d)$ para todo d, devemos ter $N(d) = \varphi(d)$ para todo d. Em particular, $N(p-1) = \varphi(p-1) > 0 \Rightarrow$ existem raízes primitivas módulo p ❑

PROBLEMAS

1) Prove que existem infinitos números primos congruentes a 3 módulo 4.
2) Determine todos os n naturais tais que $(2^n - 1)/n$ é inteiro.
3) Determine todos os n naturais tais que $(2^n + 1)/n^2$ é inteiro.
4) Prove que se a e b são naturais e $(a^2 + b^2) / (ab + 1)$ é inteiro então $(a^2 + b^2) / (ab + 1)$ é quadrado perfeito.
5) Sejam $a, n \in \mathbb{N}^*$. Considere a sequência (x_n) definida por $x_1 = a$, $x_{k+1} = a^{x_k}$, $\forall\, k \in \mathbb{N}$. Mostre que existe $N \in \mathbb{N}$ tal que $x_{k+1} \equiv x_k$ (módulo n), para todo $k \ge N$.

Obs.: Os problemas 3 e 4 foram propostos na 31ª. e na 29ª. Olimpíada Internacional de Matemática (1990 e 1988) respectivamente.