Congruências e aritmética módulo n

Carlos Gustavo Moreira - IMPA

1 Congruências

Sejam $a, b, n \in \mathbb{Z}$. Dizemos que a *é congruente a* b *módulo* n, e escrevemos $a \equiv b \pmod{n}$, se $n|b-a$. Como a congruência módulo 0 é a igualdade e quaisquer inteiros são côngruos módulo 1, em geral estamos interessados em $n > 1$.

Proposição 1.7: *Para quaisquer* $a, a', b, b', c, n \in \mathbb{Z}$ *temos:*

(a) $a \equiv a \pmod{n}$;

(b) *se* $a \equiv b \pmod{n}$ *então* $b \equiv a \pmod{n}$;

(c) *se* $a \equiv b \pmod{n}$ *e* $b \equiv c \pmod{n}$ *então* $a \equiv c \pmod{n}$;

(d) *se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$ *então* $a + b \equiv a' + b' \pmod{n}$;

(e) *se* $a \equiv a' \pmod{n}$ *então* $-a \equiv -a' \pmod{n}$;

(f) *se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$ *então* $a \cdot b \equiv a' \cdot b' \pmod{n}$.

Dem: Para o item (a) basta observar que $n|a-a=0$. Em (b), se $n|b-a$ então $n|a-b=-(b-a)$. Em (c), se $n|b-a$ e $n|c-b$ então $n|c-a=(c-b)+(b-a)$. Em (d), se $n|a'-a$ e $n|b'-b$ então $n|(a'+b')-(a+b)=(a'-a)+(b'-b)$. Em (e), se $n|a'-a$ então $n|(-a')-(-a)=-(a'-a)$. Em (f), se $n|a'-a$ e $n|b'-b$ então $n|a'b'-ab=a'(b'-b)+b(a'-a)$. □

Os itens (a), (b) e (c) da proposição acima dizem, nesta ordem, que a relação $\equiv \pmod{n}$ ("ser côngruo módulo n") é uma relação reflexiva, simétrica e transitiva. Relações satisfazendo estas três propriedades são chamadas *relações de equivalência*. Dada uma relação de equivalência $\sim$ sobre um conjunto X e um elemento $x \in X$ definimos a *classe de equivalência* $\overline{x}$ de x como

$$\overline{x} = \{y \in X | y \sim x\};$$

observe que $x \sim y$ se e somente se $\overline{x} = \overline{y}$. As classes de equivalência formam uma partição de X, i.e., uma coleção de subconjuntos não vazios e disjuntos de X cuja união é X. O conjunto $\{\overline{x} | x \in X\}$ das classes de equivalência é chamado o *quociente* de X pela relação de equivalência $\sim$ e é denotado por $X/\sim$.

Aplicando esta construção geral ao nosso caso, definimos o quociente $\mathbb{Z}/(\equiv \pmod{n})$, chamado por simplicidade de notação de $\mathbb{Z}/(n)$, $\mathbb{Z}/n\mathbb{Z}$ ou às vezes $\mathbb{Z}_n$. Dado $a \in \mathbb{Z}$, a definição de $\overline{a}$ como um subconjunto de $\mathbb{Z}$ raramente será importante: o importante é sabermos que $\overline{a} = \overline{a'}$ se e somente se $a \equiv a' \pmod{n}$. Se $n > 0$, a divisão euclidiana diz que todo inteiro a é côngruo a um

único inteiro a' com $0 \leq a' < n$; podemos reescrever este fato na nosso nova linguagem como

$$\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Quando não houver possibilidade de confusão omitiremos as barras e chamaremos os elementos de $\mathbb{Z}/(n)$ simplesmente de $0, 1, \ldots, n-1$.

Os itens (d), (e) e (f) da proposição dizem que as operações de soma, diferença e produto são compatíveis com a relação de congruência. É esta propriedade que torna congruências tão úteis, nos possibilitando fazer contas módulo n. Podemos por exemplo escrever

$$\begin{aligned} 196883 &= 1 \cdot 10^5 + 9 \cdot 10^4 + 6 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0 \\ &\equiv 1 \cdot 1^5 + 9 \cdot 1^4 + 6 \cdot 1^3 + 8 \cdot 1^2 + 8 \cdot 1^1 + 3 \cdot 1^0 \\ &= 1 + 9 + 6 + 8 + 8 + 3 \\ &= 35 \\ &\equiv 8 \pmod 9, \end{aligned}$$

já que $10 \equiv 1 \pmod 9$ (mostrando assim porque funciona o conhecido critério de divisibilidade por 9). Uma formulação mais abstrata da mesma idéia é dizer que as operações $+$ e $\cdot$ *passam ao quociente*, i.e., que podemos definir

$$+ : \mathbb{Z}/(n) \times \mathbb{Z}/(n) \to \mathbb{Z}/(n), \qquad \cdot : \mathbb{Z}/(n) \times \mathbb{Z}/(n) \to \mathbb{Z}/(n)$$

por $\overline{a} + \overline{b} = \overline{a+b}$ e $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. A dúvida à primeira vista seria se a escolha de a e b não afeta a resposta: afinal existem infinitos inteiros a' e b' com $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. Os itens (d) e (f) da proposição são exatamente o que precisamos: eles nos dizem que nestas condições $\overline{a+b} = \overline{a'+b'}$ e $\overline{a \cdot b} = \overline{a' \cdot b'}$.

Proposição 1.8: *Sejam $a, n \in \mathbb{Z}$, $n > 0$. Então existe $b \in \mathbb{Z}$ com $ab \equiv 1 \pmod n$ se e somente se $(a, n) = 1$.*

Dem: Se $ab \equiv 1 \pmod n$ temos $nk = 1 - ab$ para algum k, donde $(a, n) | ab + nk = 1$ e $(a, n) = 1$. Se $(a, n) = 1$ temos $ax + ny = 1$ para certos inteiros x e y, donde $ax \equiv 1 \pmod n$. □

Dizemos portanto que a é *invertível* [1] módulo n quando $(a, n) = 1$ e chamamos b com $ab \equiv 1 \pmod n$ de *inverso* de a módulo n. O inverso é sempre único módulo n: se $ab \equiv ab' \equiv 1 \pmod n$ temos $b \equiv ab^2 \equiv abb' \equiv b' \pmod n$.

Corolário 1.9: *Se $(a, n) = 1$ e $ab \equiv ab' \pmod n$ então $b \equiv b' \pmod n$.*

Dem: Basta escrever $b \equiv abc \equiv ab'c \equiv b' \pmod n$ onde c é o inverso de a módulo n. □

Definimos $(\mathbb{Z}/(n))^* \subset \mathbb{Z}/(n)$ por

$$(\mathbb{Z}/(n))^* = \{\overline{a}; (a, n) = 1\}.$$

Observe que o produto de elementos de $(\mathbb{Z}/(n))^*$ é sempre um elemento de $(\mathbb{Z}/(n))^*$ (corolário 1.5).

[1] Alguns autores preferem escrever *inversível*. Os interessados em discutir esta questão ortográfica devem escrever para o Prof. Zoroastro Azambuja, IMPA, Estr. D. Castorina 110, Rio de Janeiro, RJ

Estrada Dona Castorina, 110 Rio de Janeiro - Brasil 22460-320 Fone: 55 21 2529 5000/5284 Fax: 55 21 2512 4115
http://www.impa.br

Teorema 1.10: (Teorema Chinês dos restos) *Se $(m,n)=1$ então*

$$f:\mathbb{Z}/(mn)\to\mathbb{Z}/(m)\times\mathbb{Z}/(n)$$
$$\overline{a}\mapsto(\overline{a},\overline{a})$$

é uma bijeção. Além disso, a imagem por f de $(\mathbb{Z}/(mn))^*$ é $(\mathbb{Z}/(m))^*\times(\mathbb{Z}/(n))^*$.

Note que cada $\overline{a}$ na definição de f é tomado em relação a um módulo diferente. A função está bem definida pois $a \bmod mn$ determina $a \bmod m$ e $a \bmod n$.

Dem: Como $\mathbb{Z}/(mn)$ e $\mathbb{Z}/(m)\times\mathbb{Z}/(n)$ têm mn elementos cada, para provar que f é bijetiva basta verificar que f é injetiva. E, de fato, se $a\equiv a' \pmod m$ e $a\equiv a' \pmod n$ então $m|(a-a')$ e $n|(a-a')$, donde $mn|(a-a')$ e $a\equiv a' \pmod{mn}$. A imagem de $(\mathbb{Z}/(mn))^*$ é $(\mathbb{Z}/(m))^*\times(\mathbb{Z}/(n))^*$ pois $(a,mn)=1$ se e somente se $(a,m)=(a,n)=1$. □

Dados inteiros $m_1,m_2,\ldots,m_r$, dizemos que estes inteiros são *primos entre si* se $(m_i,m_j)=1$ para quaiquer $i\neq j$.

Corolário 1.11: *Se $m_1,m_2,\ldots,m_r$ são inteiros primos entre si. Então*

$$f:\mathbb{Z}/(m_1m_2\cdots m_r)\to\mathbb{Z}/(m_1)\times\mathbb{Z}/(m_2)\cdots\mathbb{Z}/(m_r)$$
$$\overline{a}\mapsto(\overline{a},\overline{a},\ldots,\overline{a})$$

é uma bijeção.

Dem: Basta aplicar o teorema anterior r vezes. □

A aplicação mais comum deste teorema é para garantir que existe a com $a\equiv a_i \pmod{m_i}$ onde a_i são inteiros dados quaisquer.

Exemplo 1. *Uma potência não trivial é um número da forma m^k, onde m, k são inteiros maiores do que ou iguais a 2. Dado $n\in\mathbb{N}$, prove que existe um conjunto $A\subset\mathbb{N}$ com n elementos tal que para todo subconjunto $B\subset A$ não vazio, $\sum_{x\in B} x$ é uma potência não trivial. Em outras palavras, se $A=\{x_1,x_2,\ldots,x_n\}$ então todas as somas $x_1,x_2,\ldots,x_n$, $x_1+x_2,x_1+x_3,\ldots,x_{n-1}+x_n,\ldots,x_1+x_2+\cdots+x_n$ são potências não triviais.*

SOLUÇÃO: Vamos provar a existência de um tal conjunto por indução em n. Para $n=1$, $A=\{4\}$ é solução e, para $n=2$, $A=\{9,16\}$ é solução. Suponha agora 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 $\lambda=\text{mmc}\{k_B \mid B\subset A, B\neq\emptyset\}$, o mínimo múltiplo comum de todos os expoentes k_B. Para cada $B\subset A$, $B\neq\emptyset$, associamos um número primo $p_B>\lambda$, de forma que $B_1\neq B_2$ implica $p_{B_1}\neq p_{B_2}$. Pelo teorema chinês dos restos existe um natural r_B com

$$\begin{aligned} r_B &\equiv 0 \pmod{p_X} \text{ para todo subconjunto } X\subset A,\ X\neq B\\ \lambda\cdot r_B &\equiv -1 \pmod{p_B}. \end{aligned}$$

Estrada Dona Castorina, 110 Rio de Janeiro - Brasil 22460-320 Fone: 55 21 2529 5000/5284 Fax: 55 21 2512 4115
http://www.impa.br

(λ é invertível módulo p_B). Tomemos

$$c = \prod_{\substack{X \subset A \\ X \neq \emptyset}} (1 + m_X^{k_X})^{\lambda r_X}$$

e vamos mostrar que $\tilde{A} = \{cx_1, cx_2, \ldots, cx_n, c\}$ continua a satisfazer as condições do enunciado.

Dado $B' \subset \{cx_1, cx_2, \ldots, cx_n\}$, temos que $B' = \{cx \mid x \in B\}$ para algum $B \subset A$. Como c é uma potência λ-ésima, c também é uma potência k_B-ésima, portanto, $\sum_{x \in B'} x = cm_B^{k_B}$ será uma potência k_B-ésima para todo $B' \neq \emptyset$. Além disso, para subconjuntos de $\tilde{A}$ da forma $B' \cup \{c\}$, temos

$$\sum_{x \in B' \cup \{c\}} x = c \cdot (1 + m_B^{k_B}) = \Big(\prod_{\substack{X \subset A \\ X \neq \emptyset, B}} (1 + m_X^{k_X})^{\lambda r_X} \Big) (1 + m_B^{k_B})^{\lambda r_B + 1},$$

que é uma potência p_B-ésima, pois $\lambda r_B + 1$ e r_X $(X \neq B)$ são múltiplos de p_B. □

2 A função de Euler e o pequeno teorema de Fermat

Definimos $\varphi(n) = |(\mathbb{Z}/(n))^*|$ (onde $|X|$ denota o número de elementos de X). A função φ é conhecida como a *função de Euler*. Temos $\varphi(1) = \varphi(2) = 1$, e, para $n > 2$, $1 < \varphi(n) < n$. Se p é primo, $\varphi(p) = p - 1$; mais geralmente $\varphi(p^k) = p^k - p^{k-1}$ pois $(a, p^k) = 1$ se e somente se a não é múltiplo de p e há p^{k-1} múltiplos de p no intervalo $0 \leq a < p^k$.

Dizemos que os n números inteiros $a_1, a_2, \ldots, a_n$ formam um *sistema completo de resíduos* (ou s.c.r.) módulo n se $\{\overline{a_1}, \overline{a_2}, \ldots \overline{a_n}\} = \mathbb{Z}/(n)$, isto é, se os a_i representam todas as classes de congruência módulo n. Por exemplo, 0, 1, 2, $\ldots n-1$ formam um s.c.r. módulo n. Equivalentemente, podemos dizer que $a_1, a_2, \ldots, a_n$ formam um s.c.r. módulo n se e somente se $a_i \equiv a_j \pmod{n}$ implicar $i = j$. Os $\varphi(n)$ números inteiros $b_1, b_2, \ldots, b_{\varphi(n)}$ formam um *sistema completo de invertíveis* (s.c.i.) módulo n se

$$\{\overline{b_1}, \overline{b_2}, \ldots \overline{b_{\varphi(n)}}\} = (\mathbb{Z}/(n))^*,$$

isto é, se os b_i representam todas as classes de congruências invertíveis módulo n. Também equivalentemente, $b_1, b_2, \ldots, b_{\varphi(n)}$ formam um s.c.i. módulo n se e somente se $(b_i, n) = 1$ para todo i e $a_i \equiv a_j \pmod{n}$ implicar $i = j$.

Proposição 1.12: *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.*

Prova: Se $qa_i + r \equiv qa_j + r \pmod{n}$ então $n | q(a_i - a_j)$ e $a_i \equiv a_j \pmod{n}$, donde $i = j$; com isto provamos que $qa_1 + r, qa_2 + r, \ldots, qa_n + r$ formam um s.c.r..

Estrada Dona Castorina, 110 Rio de Janeiro - Brasil 22460-320 Fone: 55 21 2529 5000/5284 Fax: 55 21 2512 4115
http://www.impa.br

Como $(q,n) = (b_i, n) = 1$, temos $(qb_i, n) = 1$. Por outro lado, se $qb_i \equiv qb_j \pmod{n}$ temos $b_i \equiv b_j \pmod{n}$ (como no parágrafo anterior) e $i = j$. Isto conclui a demonstração. □

Teorema 1.13: (Euler) *Sejam $a, n \in \mathbb{Z}$, $n > 0$, tais que $(a,n) = 1$. Então $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Prova: Seja

$$b_1, b_2, \ldots . b_{\varphi(n)}$$

um s.c.i. módulo n. Pela proposição anterior,

$$ab_1, ab_2, \ldots ab_{\varphi(n)}$$

também formam um s.c.i. módulo n. Assim,

$$b_1 \cdot b_2 \cdots b_{\varphi(n)} \equiv ab_1 \cdot ab_2 \cdots ab_{\varphi(n)} \pmod{n}$$

pois módulo n os dois lados têm os mesmos fatores a menos de permutação. Mas isto pode ser reescrito como

$$a^{\varphi(n)}(b_1 \cdot b_2 \cdots b_{\varphi(n)}) \equiv 1 \cdot (b_1 \cdot b_2 \cdots b_{\varphi(n)}) \pmod{n}$$

e pelo corolário 1.9 isto implica $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Corolário 1.14: (Pequeno Teorema de Fermat) *Se p é primo então, para todo inteiro a, $a^p \equiv a \pmod{p}$.*

Prova: Se $p|a$, então $a^p \equiv a \equiv 0 \pmod{p}$. Caso contrário, $\varphi(p) = p - 1$, $a^{p-1} \equiv 1 \pmod{p}$ e novamente $a^p \equiv a \pmod{p}$. □

Outra demonstração do pequeno teorema de Fermat é por indução em a usando o binômio de Newton e algumas propriedades de números binomiais. Se $0 < i < p$ temos

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \equiv 0 \pmod{p}$$

pois há um fator p no numerador que não pode ser cancelado com nada que apareça no denominador. Os casos $a = 0$ e $a = 1$ do teorema são triviais. Supondo válido o teorema para a, temos

$$\begin{aligned}(a+1)^p &= a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1 \\ &\equiv a^p + 1 \\ &\equiv a + 1 \pmod{p}\end{aligned}$$

e a indução está completa.

Corolário 1.15: *Se $(m,n) = 1$ então $\varphi(mn) = \varphi(m)\varphi(n)$.*

Prova: Construimos uma bijeção entre $(\mathbb{Z}/(mn))^*$ e $(\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$, o que garante que estes conjuntos têm o mesmo número de elementos. □

Corolário 1.16: *Se*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

Estrada Dona Castorina, 110 Rio de Janeiro - Brasil 22460-320 Fone: 55 21 2529 5000/5284 Fax: 55 21 2512 4115
http://www.impa.br

com $p_1 < p_2 < \ldots < p_m$ *e* $e_i > 0$ *para todo* i *então*

$$\begin{aligned}\varphi(n) &= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_m^{e_m} - p_m^{e_m-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).\end{aligned}$$

Prova: Isto segue da fórmula que já vimos para $\varphi(p^e)$ e do corolário anterior. □

Em particular, se $n > 2$ então $\varphi(n)$ é par.

Exemplo 2. *Encontre um número* $n \in \mathbb{N}$ *tal que* $2^n > 10^{2000}$ *e* 2^n *tenha entre suas 2000 últimas casas decimais pelo menos 1000 zeros consecutivos.*

SOLUÇÃO: Sabemos que $2^{\varphi(5^{2000})} \equiv 1 \pmod{5^{2000}}$ pelo teorema de Euler-Fermat. Portanto existe $b \in \mathbb{N}$ com

$$2^{\varphi(5^{2000})} = 5^{2000}b + 1 \implies 2^{2000+\varphi(5^{2000})} = 10^{2000}b + 2^{2000}.$$

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 $2^{2000} < (2^3)^{667} < 10^{667}$. Desta forma, há pelo menos $2000 - 667 = 1333$ zeros consecutivos dentre as 2000 últimas casas decimais de $2^{2000+\varphi(5^{2000})}$ e assim $n = \varphi(5^{2000}) + 2000 = 4 \cdot 5^{1999} + 2000$ satisfaz as condições do enunciado. □

Concluímos esta seção apresentando brevemente uma aplicação do Teorema de Euler que tem particular interesse prático: a *Criptografia RSA*. Trata-se de um método de criptografia com chave pública, isto é, um método que permite a qualquer pessoa transmitir mensagens por uma via insegura (ou seja, que pode ser monitorada por espiões) de modo que, na prática, apenas o legítimo destinatário, que conhece uma *chave*, pode recuperar a mensagem original. A sigla vem dos nomes de Ron Rivest, Adi Shamir, e Leonard Adleman, que desenvolveram esse método.

Para isso, o receptor publica um inteiro N que é o produto de dois primos razoavelmente grandes p e q (aproximadamente da mesma ordem de grandeza); N é público mas a sua fatoração pq só é conhecida pelo receptor. O receptor também publica um expoente s (em geral não muito grande) com $\text{mdc}(s, (p-1)(q-1)) = 1$. O receptor calcula (usando o algoritmo de Euclides) o inverso de $s \bmod (p-1)(q-1) = \varphi(N)$, isto é, um natural $r < (p-1)(q-1)$ com $rs \equiv 1 \pmod{(p-1)(q-1)}$ (donde $rs = 1 + k\varphi(N)$, para algum natural k); esse r é chamado a *chave privada* da criptografia. Note que apesar de N e s serem públicos, não parece ser fácil calcular $\varphi(N)$ ou r (neste contexto, calcular $\varphi(N) = (p-1)(q-1)$ dado $N = pq$ é equivalente a fatorar N, i.e., a encontrar os fatores primos p e q).

Uma mensagem é um número natural $m < N$. O emissor envia (ou publica) $\tilde{m} := m^s \pmod{N}$, com $0 < \tilde{m} < N$. O receptor recupera m via

$$m \equiv \tilde{m}^r \pmod{N}.$$

Estrada Dona Castorina, 110 Rio de Janeiro - Brasil 22460-320 Fone: 55 21 2529 5000/5284 Fax: 55 21 2512 4115
http://www.impa.br

Para verificar essa equivalência, podemos observar que

$$\tilde{m}^r \equiv (m^s)^r = m^{rs} = m^{1+k(p-1)(q-1)} = m \cdot (m^{p-1})^{k(q-1)} \equiv m \pmod{p}.$$

Note que, se $p \mid m$, os dois lados são 0 mod p, e, caso contrário, $m^{p-1} \equiv 1 \pmod{p}$; analogamente $\tilde{m}^r \equiv m \pmod{q}$, donde $\tilde{m}^r \equiv m \pmod{N}$. Essas tarefas são relativamente rápidas computacionalmente, mas acredita-se que fatorar inteiros grandes é uma tarefa bem mais complicada e demorada computacionalmente, o que garante na prática a eficiência do método.

Mais adiante estudaremos equações do segundo grau em $\mathbb{Z}/(p)$; vejamos desde já um pequeno resultado deste tipo que garante que os únicos a que são seus próprios inversos módulo p são 1 e -1.

Lema 1.17: *Se p é primo então as únicas soluções de $x^2 = 1$ em $\mathbb{Z}/(p)$ são 1 e -1. Em particular,se $x \in (\mathbb{Z}/(p))^* - \{1, -1\}$ então $x^{-1} \neq x$ em $\mathbb{Z}/(p)$.*

Prova: Podemos reescrever a equação como $(x-1)(x+1) = 0$, o que torna o resultado trivial. □

Teorema 1.18: (Wilson) *Seja $n > 4$. Então $(n-1)! \equiv -1 \pmod{n}$ se n é primo e $(n-1)! \equiv 0 \pmod{n}$ se n é composto.*

Prova: Se n é composto mas não é o quadrado de um primo podemos escrever $n = ab$ com $1 < a < b < n$: neste caso tanto a quanto b aparecem em $(n-1)!$ e $(n-1)! \equiv 0 \pmod{n}$. Se $n = p^2$, $p > 2$, então p e $2p$ aparecem em $(n-1)!$ e novamente $(n-1)! \equiv 0 \pmod{n}$; isto demonstra que para todo n composto, $n > 4$, temos $(n-1)! \equiv 0 \pmod{n}$.

Se n é primo podemos escrever $(n-1)! \equiv -(2 \cdot 3 \cdots n-2) \pmod{n}$; mas pelo lema anterior podemos juntar os inversos aos pares no produto do lado direito, donde $(n-1)! \equiv -1 \pmod{n}$. □

3 Ordem e Raízes Primitivas

Dado $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, definimos a *ordem de* $\overline{a}$, denotado por $\operatorname{ord} \overline{a}$, como o menor inteiro $t > 0$ tal que $\overline{a}^t = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$. Se $a, n \in \mathbb{Z}$ com $\operatorname{mdc}(a, n) = 1$, definimos a *ordem de a módulo n*, denotado por $\operatorname{ord}_n a$, como a ordem de $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Note que pelo teorema de Euler-Fermat, temos que $\operatorname{ord}_n a \leq \varphi(n)$. Se $\operatorname{ord}_n a = \varphi(n)$, dizemos que a é *raiz primitiva módulo n*. Por exemplo, 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 $4 = \varphi(5)$.

O resultado básico mais importante sobre ordem é a seguinte

Proposição 3. *Temos que $a^t \equiv 1 \pmod{n}$ se, e só se, $\operatorname{ord}_n a \mid t$.*

Demonstração. Como $a^{\operatorname{ord}_n a} \equiv 1 \pmod{n}$, para todo $k \in \mathbb{N}$ tem-se $a^{k \operatorname{ord}_n a} \equiv 1 \pmod{n}$. Por outro lado, se $a^t \equiv 1 \pmod{n}$, pelo algoritmo da divisão existem inteiros q e r tais que $0 \leq r < \operatorname{ord}_n a$ e $t = q \operatorname{ord}_n a + r$. Portanto

$$1 \equiv a^t = a^{q \operatorname{ord}_n a + r} = (a^{\operatorname{ord}_n a})^q \cdot a^r \equiv a^r \pmod{n}$$

Ou seja, $a^r \equiv 1 \pmod{n}$. Pela minimalidade de $\operatorname{ord}_n a$, temos que $r = 0$, i.e., $\operatorname{ord}_n a \mid t$. □

Estrada Dona Castorina, 110 Rio de Janeiro - Brasil 22460-320 Fone: 55 21 2529 5000/5284 Fax: 55 21 2512 4115
http://www.impa.br

Corolário 4. $\operatorname{ord}_n a \mid \varphi(n)$.

Exemplo 5. *Demonstre que $n \mid \varphi(a^n - 1)$ para todo inteiro positivo $a > 1$.*

SOLUÇÃO: Já que $\operatorname{mdc}(a, a^n - 1) = 1$, pelo teorema de Euler-Fermat temos que $a^{\varphi(a^n-1)} \equiv 1 \pmod{a^n - 1}$; por outro lado, n é a ordem de a módulo $a^n - 1$ já que $a^n \equiv 1 \pmod{a^n - 1}$ e se $0 < t < n$ temos $0 < a^t - 1 < a^n - 1$ e assim $a^n - 1 \nmid a^t - 1$. Pela proposição, temos portanto $n \mid \varphi(a^n - 1)$. □

Exemplo 6. *Demonstre que não existe um inteiro $n > 1$ tal que $n \mid 2^n - 1$.*

SOLUÇÃO: Suponhamos o contrário; seja p o menor divisor primo de n e $r = \operatorname{ord}_p 2$. Sabemos que $2^n \equiv 1 \pmod p$ e além disso, pelo teorema de Fermat, $2^{p-1} \equiv 1 \pmod p$.

Portanto $r \mid n$ e $r \mid p - 1$, o que implica que $r \mid \operatorname{mdc}(n, p - 1)$. Mas $\operatorname{mdc}(n, p - 1) = 1$ pois p é o menor divisor primo de n e assim os divisores primos de $p - 1$ são menores que os divisores primos de n. Isto mostra que $r = 1$, isto é $2^1 \equiv 1 \pmod p$, donde $p \mid 1$, uma contradição. □

Exemplo 7. *Sejam a, m e n inteiros positivos; defina m' e n' por $m = \operatorname{mdc}(m, n) \cdot m'$ e $n = \operatorname{mdc}(m, n) \cdot n'$, de modo que $\operatorname{mdc}(m', n') = 1$. Mostre que*

$$\operatorname{mdc}(a^m + 1, a^n + 1) = \begin{cases} a^{\operatorname{mdc}(m,n)} + 1 & \text{se } m' \text{ e } n' \text{ são ímpares.} \\ 2 & \text{se } m' + n' \text{ e } a \text{ são ímpares.} \\ 1 & \text{se } m' + n' \text{ é ímpar e } a \text{ é par.} \end{cases}$$

SOLUÇÃO: Como

$$\operatorname{mdc}(a^m + 1, a^n + 1) = \operatorname{mdc}\big((a^{\operatorname{mdc}(m,n)})^{m'} + 1, (a^{\operatorname{mdc}(m,n)})^{n'} + 1\big),$$

o resultado no caso geral seguirá do caso em que $\operatorname{mdc}(m, n) = 1$. Assim, vamos supor m e n são primos entre si e seja $d = \operatorname{mdc}(a^n + 1, a^m + 1)$. Temos

$$\begin{cases} a^n \equiv -1 \pmod d \\ a^m \equiv -1 \pmod d \end{cases} \implies \begin{cases} a^{2n} \equiv 1 \pmod d \\ a^{2m} \equiv 1 \pmod d \end{cases}$$
$$\implies \operatorname{ord}_d a \mid \operatorname{mdc}(2n, 2m) = 2.$$

Assim, $a^2 \equiv 1 \pmod d$. Digamos que m seja ímpar (como estamos supondo $\operatorname{mdc}(m, n) = 1$, não podemos ter m e n ambos pares), de modo que

$$a \cdot (a^2)^{(m-1)/2} = a^m \equiv -1 \pmod d \implies a \equiv -1 \pmod d$$
$$\iff d \mid a + 1.$$

Se n é ímpar também, então $d = a + 1$ já que $a + 1 \mid a^m + 1$ e $a + 1 \mid a^n + 1$ neste caso (utilize a fatoração $a^m + 1 = (a + 1)(a^{m-1} - a^{m-2} + a^{m-3} - \cdots + 1)$ ou a implicação $a \equiv -1 \pmod{a + 1} \implies a^m \equiv -1 \pmod{a + 1}$). Por outro lado, se n é par, temos

$$(a^2)^{n/2} = a^n \equiv -1 \pmod d \implies 1 \equiv -1 \pmod d$$
$$\implies d = 1 \text{ ou } d = 2.$$

O caso $d = 2$ ocorre se, e só se, $a^m + 1$ e $a^n + 1$ são ambos pares, ou seja, quando a é ímpar. Isto encerra a análise de casos e com isso o problema. □

Estrada Dona Castorina, 110 Rio de Janeiro - Brasil 22460-320 Fone: 55 21 2529 5000/5284 Fax: 55 21 2512 4115
http://www.impa.br

Uma outra caracterização de raiz primitiva é dada pela

Proposição 8. *O número a é raiz primitiva módulo n se, e somente se, $\{\overline{a}^t, t \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^\times$.*

Demonstração. Para todo $a \in \mathbb{Z}$ com $\text{mdc}(a, n) = 1$ temos $\{\overline{a}^t, t \in \mathbb{N}\} \subset (\mathbb{Z}/n\mathbb{Z})^\times$. Note que $\{\overline{a}^t, t \in \mathbb{N}\} = \{\overline{1}, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{\text{ord}_n a - 1}\}$ é um conjunto com $\text{ord}_n a$ elementos. De fato, para qualquer $t \in \mathbb{N}$ temos $\overline{a}^t = \overline{a}^r$ onde r é o resto na divisão de t por $\text{ord}_n a$; por outro lado, os elementos $\overline{1}, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{\text{ord}_n a - 1}$ são distintos pois caso $\overline{a}^i = \overline{a}^j$ com $0 \leq i < j < \text{ord}_n a$, então $\overline{a}^{j-i} = \overline{1}$ com $0 < j - i < \text{ord}_n a$, o que é absurdo.

Assim, $\{\overline{a}^t, t \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^\times$ se, e só se, $\text{mdc}(a, n) = 1$ e $\text{ord}_n a = \varphi(n)$, isto é, se, e só se, a é uma raiz primitiva módulo n. □

Referências

[1] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.

Estrada Dona Castorina, 110 Rio de Janeiro - Brasil 22460-320 Fone: 55 21 2529 5000/5284 Fax: 55 21 2512 4115
http://www.impa.br

Estrada Dona Castorina, 110 Rio de Janeiro - Brasil 22460-320 Fone: 55 21 2529 5000/5284 Fax: 55 21 2512 4115
http://www.impa.br