Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 7

Ordens e raízes primitivas

1 Polinômios

Dado um anel comutativo K, definimos o anel comutativo $K[x]$ como sendo o conjunto das expressões da forma $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ com $a_i \in K$, chamados de *polinômios* com coeficientes em K. A soma e o produto em $K[x]$ são definidos da maneira usual: dados $f(x) = \sum_i a_ix^i$ e $g(x) = \sum_i b_ix^i$ elementos de $K[x]$ temos

$$f(x) + g(x) \stackrel{\text{def}}{=} \sum_i (a_i + b_i)x^i;$$
$$f(x) \cdot g(x) \stackrel{\text{def}}{=} \sum_k c_kx^k \text{ onde } c_k = \sum_{i+j=k} a_ib_j.$$

Definimos o *grau* $\deg f(x)$ de um polinômio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ como sendo o maior i tal que $a_i \neq 0$; o grau do polinômio nulo 0 é definido como sendo $-\infty$. Tal convenção visa a tornar válidas as seguintes identidades para todos os polinômios $f(x), g(x) \in K[x]$:

$$\deg\big(f(x) \cdot g(x)\big) = \deg f(x) + \deg g(x) \qquad \text{e}$$
$$\deg\big(f(x) + g(x)\big) \leq \max\{\deg f(x), \deg g(x)\}.$$

O coeficiente do termo de maior grau de um polinômio é chamado de *coeficiente líder*. Um polinômio cujo coeficiente líder é igual a 1 é chamado de *mônico*.

Observe que nas definições acima x é um símbolo formal e não um elemento de K. Apesar disso, cada polinômio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ define uma *função polinomial*

$$f\colon K \to K$$
$$c \mapsto f(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n$$

também chamada de f. A distinção entre um polinômio e uma função polinomial é bem ilustrada pelo polinômio $f(x) = x^p - x \in (\mathbb{Z}/(p))[x]$: este polinômio

é não nulo pois seus coeficientes são não nulos, mas para todo $c \in \mathbb{Z}/(p)$ temos $f(c) = 0$ pelo pequeno teorema de Fermat. Dado um polinômio $f(x) \in K[x]$, qualquer $c \in K$ tal que $f(c) = 0$ é chamado de *raiz* ou *zero* de $f(x)$.

Como veremos nesta seção, polinômios guardam muitas semelhanças com números inteiros. Por exemplo, podemos definir divisibilidade de polinômios de maneira completamente análoga: $d(x) \mid f(x)$ em $K[x]$ se, e só se, existe $g(x) \in K[x]$ tal que $f(x) = d(x) \cdot g(x)$. Temos também uma generalização da divisão euclidiana:

Proposição 1 (Algoritmo da divisão)**.** *Seja K um corpo. Dados polinômios $f(x), g(x) \in K[x]$, com $g(x) \neq 0$, existem $q(x), r(x) \in K[x]$ (chamados respectivamente de* quociente *e* resto *da divisão de $f(x)$ por $g(x)$), unicamente determinados, tais que*

$$f(x) = q(x) \cdot g(x) + r(x) \quad \textit{com} \quad \deg r(x) < \deg g(x).$$

Demonstração. Sejam $n = \deg f(x)$ e $m = \deg g(x)$. Para demonstrar a existência de $q(x)$ e $r(x)$, procederemos por indução sobre n. Note que se $m > n$, então basta tomar $q(x) = 0$ e $r(x) = f(x)$, logo podemos supor que $m \leq n$. Se $n = m = 0$, então $f(x) = a$ e $g(x) = b$ são ambos constantes não nulas, logo basta tomar $q(x) = a/b$ e $r(x) = 0$ neste caso.

Agora suponha que $n \geq 1$. Escreva $f(x) = a_n x^n + f_1(x)$ e $g(x) = b_m x^m + g_1(x)$ com $a_n \neq 0$, $b_m \neq 0$ e $\deg f_1(x) < n$, $\deg g_1(x) < m$. Observemos que o polinômio $f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = f_1(x) - \frac{a_n}{b_m} x^{n-m} g_1(x)$ é de grau menor que n. Por hipótese de indução existem dois polinômios $q(x)$ e $r(x)$ tais que

$$f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = q(x)g(x) + r(x) \quad \text{com} \quad \deg r(x) < \deg g(x).$$

Logo podemos escrever $f(x) = (\frac{a_n}{b_m} x^{n-m} + q(x)) \cdot g(x) + r(x)$, que era o que se queria demonstrar.

Para demonstrar que os polinômios $q(x)$ e $r(x)$ são únicos, suponha que

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

com $q_1(x) \neq q_2(x)$ e $\deg r_1(x), \deg r_2(x) < \deg g(x)$. Então $r_2(x) - r_1(x) = (q_1(x) - q_2(x))g(x) \neq 0$ é um múltiplo de $g(x)$ de grau estritamente menor do que $\deg g(x)$, o que é um absurdo. □

Corolário 2. *Seja K um corpo, $f(x) \in K[x]$ e $a \in K$. Então*

$$x - a \mid f(x) \iff f(a) = 0.$$

Demonstração. Como $\deg(x - a) = 1$, dividindo $f(x)$ por $x - a$ temos que $f(x) = (x - a)q(x) + r$ com $r \in K$. Assim, substituindo x por a, temos que $f(a) = r$ donde o resultado segue. □

Proposição 3. *Seja K um corpo. Um polinômio $f(x) \in K[x]$ não nulo de grau n tem no máximo n raízes em K.*

Demonstração. A demonstração é feita por indução em $n = \deg f(x)$; os casos $n = 0$ e $n = 1$ são triviais. Se $f(x)$ tivesse $n+1$ raízes distintas $a_1, \ldots, a_{n+1}$, então $f(x) = (x - a_{n+1})g(x)$ para algum $g(x) \in K[x]$ pelo corolário anterior. Assim, para $i \neq n+1$, teríamos $0 = f(a_i) = (a_i - a_{n+1})g(a_i) \implies g(a_i) = 0$ pois $(a_i - a_{n+1}) \neq 0$ é invertível em K. Logo $g(x)$, de grau $n-1$, teria n raízes distintas $a_1, \ldots, a_n$, contradizendo a hipótese de indução. □

Note que o teorema anterior é falso se K não é um corpo. Por exemplo, o polinômio $f(x) = x^2 - 1 \in \mathbb{Z}/8\mathbb{Z}[x]$ tem 4 raízes em $\mathbb{Z}/8\mathbb{Z}$, a saber $\overline{1}, \overline{3}, \overline{5}, \overline{7}$.

Vejamos uma aplicação dos resultados anteriores quando $K = \mathbb{Z}/(p)$, p primo. A primeira é uma nova demonstração do teorema de Wilson:

Teorema 4. *Seja p um primo. Considere a função simétrica elementar σ_i em $1, 2, \ldots, p-1$ dada pela soma de todos os $\binom{p-1}{i}$ produtos de i termos distintos dentre $1, 2, \ldots, p-1$:*

$$\begin{aligned}
\sigma_1 &= 1 + 2 + \cdots + (p-1) \\
\sigma_2 &= 1 \cdot 2 + 1 \cdot 3 + \cdots + (p-2)(p-1) \\
&\vdots \\
\sigma_{p-1} &= 1 \cdot 2 \cdot \ldots \cdot (p-1).
\end{aligned}$$

Então $\sigma_1, \ldots, \sigma_{p-2}$ são todos múltiplos de p e $\sigma_{p-1} = (p-1)! \equiv -1 \pmod{p}$ (teorema de Wilson).

Demonstração. Pelo teorema de Fermat e pela proposição anterior, temos que $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ são todas as raízes de $x^{p-1} - \overline{1}$ em $\mathbb{Z}/(p)$. Logo aplicando o corolário e comparando coeficientes líderes obtemos a fatoração

$$x^{p-1} - \overline{1} = (x - \overline{1})(x - \overline{2}) \cdot \ldots \cdot (x - \overline{p-1}).$$

Mas o polinômio do lado direito é igual a $x^{p-1} - \overline{\sigma}_1 x^{p-2} + \overline{\sigma}_2 x^{p-3} - \cdots + (-1)^{p-1}\overline{\sigma}_{p-1}$. Comparando coeficientes, obtemos o resultado. □

2 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 5. *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., $\operatorname{ord}_n a \mid t$. □

Corolário 6. $\operatorname{ord}_n a \mid \varphi(n)$.

Exemplo 7. *Demonstrar 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 8. *Demonstrar 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 9. *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 $\text{mdc}(m,n) = 1$, não podemos ter m e n ambos pares), de modo que

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

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

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

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. □

Uma outra caracterização de raiz primitiva é dada pela

Proposição 10. *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 $0 \le i < j < \text{ord}_n a$, 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. □

Corolário 11. *Se m divide n e a é raiz primitiva módulo n, então a é raiz primitiva módulo m.*

Demonstração. Vamos mostrar que o mapa natural $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ que leva $x \bmod n$ em $x \bmod m$ é sobrejetor: de fato, se $\text{mdc}(b,m) = 1$ e Q é o produto dos primos que dividem n mas não dividem m, temos $\text{mdc}(m,Q) = 1$, e logo existem x, y inteiros com $mx + Qy = 1$. Considere $\tilde{b} := b + mx(1-b) \equiv b \pmod{m}$. Temos então $\text{mdc}(\tilde{b}, m) = \text{mdc}(b,m) = 1$, e, como $\tilde{b} := b + mx(1-b) = b + (1-Qy)(1-b) = 1 - Qy(1-b) \equiv 1 \pmod{Q}$, temos $\text{mdc}(\tilde{b}, Q) = 1$, e logo $\text{mdc}(\tilde{b}, n) = 1$ (e $\tilde{b}$ é levado em b pelo mapa natural acima). Assim, temos que se as potências de $a \bmod n$ cobrem todo o $(\mathbb{Z}/n\mathbb{Z})^\times$, então as potências de $a \bmod m$ também cobrem todo o $(\mathbb{Z}/m\mathbb{Z})^\times$. Pela proposição, isto implica o corolário. □

Raízes primitivas são muito úteis em diversas questões de Teoria dos Números. Entretanto elas nem sempre existem para qualquer módulo n. O resto desta seção é dedicado a provar o seguinte importante

Teorema 12. *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.*

A demonstração deste teorema é longa e é composta de vários passos. Começamos com a seguinte

Proposição 13. *Se $k \geq 3$, então não existe nenhuma raiz primitiva módulo 2^k.*

Demonstração. Pelo corolário anterior, basta provar que não existe raiz primitiva módulo 8, e isso segue do fato de que se $\text{mdc}(a, 8) = 1$, isto é, $a = 2r + 1$, $r \in \mathbb{N}$, então $a^2 = 4r(r + 1) + 1 \equiv 1 \pmod 8$ (sendo $r(r + 1)$ par, visto que é o produto de dois números consecutivos). Assim, não há elemento de ordem $\varphi(8) = 4$ módulo 8. □

Proposição 14. *Se $n = ab$, com $a \geq 3$ e $b \geq 3$ inteiros tais que $\text{mdc}(a, b) = 1$, então não existe raiz primitiva módulo n.*

Demonstração. Como $\varphi(n) = \varphi(a)\varphi(b)$ e $a \geq 3$ e $b \geq 3$, segue que $\varphi(a)$ e $\varphi(b)$ são pares (verifique!). Se $\text{mdc}(k, n) = 1$, então temos

$$k^{\varphi(n)/2} = (k^{\varphi(b)/2})^{\varphi(a)} \equiv 1 \pmod a \qquad \text{e}$$
$$k^{\varphi(n)/2} = (k^{\varphi(a)/2})^{\varphi(b)} \equiv 1 \pmod b.$$

Assim, $k^{\varphi(n)/2} \equiv 1 \pmod n$ e portanto $\text{ord}_n k \leq \varphi(n)/2 < \varphi(n)$ para todo k primo com n. □

Proposição 15. *Se p é um número primo e $a \in \mathbb{Z}$ é uma raiz primitiva módulo p, então a ou $a + p$ é raiz primitiva módulo p^2.*

Demonstração. Por hipótese, $\text{ord}_p a = \text{ord}_p(a + p) = \varphi(p) = p - 1$. Portanto $p - 1 \mid \text{ord}_{p^2} a$, pois $a^t \equiv 1 \pmod{p^2}$ implica $a^t \equiv 1 \pmod p$. Além disso, como $\text{ord}_{p^2} a \mid \varphi(p^2) = p(p - 1)$, devemos ter $\text{ord}_{p^2} a = p - 1$ ou $\text{ord}_{p^2} a = p(p - 1) = \varphi(p^2)$. Do mesmo modo, $\text{ord}_{p^2}(a+p) = p-1$ ou $\text{ord}_{p^2}(a+p) = p(p-1) = \varphi(p^2)$. Basta provar, portanto, que $\text{ord}_{p^2} a \neq p - 1$ ou $\text{ord}_{p^2}(a + p) \neq p - 1$. Suponha que $\text{ord}_{p^2} a = p - 1$. Portanto $a^{p-1} \equiv 1 \pmod{p^2}$ e assim

$$\begin{aligned}(a + p)^{p-1} &= a^{p-1} + \binom{p-1}{1} a^{p-2}p + \binom{p-1}{2} a^{p-3}p^2 + \cdots \\ &\equiv 1 - pa^{p-2} \pmod{p^2}.\end{aligned}$$

Portanto $(a + p)^{p-1}$ não é congruente a 1 módulo p^2, pois p^2 não divide pa^{p-2} (lembre-se de que $\text{mdc}(a, p) = 1$), donde $\text{ord}_{p^2}(a + p) \neq p - 1$. □

Proposição 16. *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. Como $a^{p-1} \equiv 1 \pmod p$, mas a^{p-1} não é congruente a 1 módulo p^2 (já que a é raiz primitiva módulo p^2), temos $a^{p-1} = 1+b_1p$, 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 $k \geq 1$. De fato, para $k \geq 1$ e $p > 2$ primo,

$$\begin{aligned} a^{p^k(p-1)} = (1 + b_k p^k)^p &= 1 + \binom{p}{1} b_k p^k + \binom{p}{2} b_k^2 p^{2k} + \cdots \\ &= 1 + p^{k+1}(b_k + pt) \end{aligned}$$

para algum $t \in \mathbb{Z}$ e assim $b_{k+1} = b_k + pt$ também não é divisível por p pois $p \nmid b_k$.

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. Como $a^{\mathrm{ord}_{p^{k+1}} a} \equiv 1 \pmod{p^{k+1}} \implies a^{\mathrm{ord}_{p^{k+1}} a} \equiv 1 \pmod{p^k}$ temos

$$p^{k-1}(p-1) = \varphi(p^k) = \mathrm{ord}_{p^k} a \mid \mathrm{ord}_{p^{k+1}} a \mid \varphi(p^{k+1}) = p^k(p-1).$$

Portanto $\mathrm{ord}_{p^{k+1}} a = p^{k-1}(p-1)$ ou $\mathrm{ord}_{p^{k+1}} a = p^k(p-1) = \varphi(p^{k+1})$, mas o primeiro caso é impossível pois $a^{p^{k-1}(p-1)} = 1 + b_k p^k$ com $p \nmid b_k$. Logo $\mathrm{ord}_{p^{k+1}} a = \varphi(p^{k+1})$ e a é raiz primitiva módulo p^{k+1}. □

Por exemplo 2 é raiz primitiva módulo 5^k para todo $k \geq 1$. De fato, 2 é raiz primitiva módulo 5 e, como $2^4 = 16 \not\equiv 1 \pmod{25}$, 2 é raiz primitiva módulo $25 = 5^2$ também. Portanto, pela proposição anterior, 2 é raiz primitiva módulo 5^k para todo $k \geq 1$.

Proposição 17. *Se p é primo ímpar e a é um inteiro ímpar tal que a é raiz primitiva módulo p^k, então a é raiz primitiva módulo $2p^k$. Em particular, se a é raiz primitiva qualquer módulo p^k, então a ou $a + p^k$ é raiz primitiva módulo $2p^k$ (pois um deles é ímpar).*

Demonstração. Temos, como nas provas acima, $\varphi(p^k) = \mathrm{ord}_{p^k} a \mid \mathrm{ord}_{2p^k} a$ e $\mathrm{ord}_{2p^k} a \mid \varphi(2p^k) = \varphi(p^k)$, logo $\mathrm{ord}_{2p^k} a = \varphi(2p^k)$. □

Para completar a prova do teorema 12, falta provar que se p é primo ímpar, então existe raiz primitiva módulo p. Para isto, precisamos de dois lemas.

Lema 18. *$\sum_{d|n} \varphi(d) = n$ para todo $n \in \mathbb{N}$.*

Demonstração. Seja d um divisor de n. A quantidade de a's tais que $1 \leq a \leq n$ e $d = \mathrm{mdc}(n, a)$ é igual a $\varphi(\frac{n}{d})$ pois $d = \mathrm{mdc}(n, a) \iff d \mid a$ e $1 = \mathrm{mdc}(\frac{n}{d}, \frac{a}{d})$. Como $\varphi(\frac{n}{d})$ conta justamente a quantidade de inteiros entre 1 e $\frac{n}{d}$ (inclusive) que são primos com $\frac{n}{d}$, temos que $\sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$ conta a quantidade de números a entre 1 e n (inclusive), particionados segundo os valores de $\mathrm{mdc}(a, n)$. □

Lema 19. *Seja p um primo e d um divisor de $p - 1$. Defina $N(d)$ como a quantidade de elementos $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ com $\mathrm{ord}\,\overline{a} = d$. Então $N(d) \leq \varphi(d)$.*

Demonstração. Podemos supor que $N(d) > 0$, logo existe a tal que $\mathrm{ord}_p a = d$. Logo $\overline{a}^d = \overline{1}$ e, para $0 \leq k < d$, as classes de a^k são todas distintas módulo p. Como $(\overline{a}^k)^d = 1$ e 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 $\overline{a}^k$, $0 \leq k < d$. Por outro lado, se $\mathrm{ord}_p\, a^k = d$, então $\mathrm{mdc}(k,d) = 1$, pois caso $r = \mathrm{mdc}(k,d) > 1$, então $(a^k)^{d/r} = (a^d)^{k/r} \equiv 1 \pmod{p}$, logo $\mathrm{ord}_p(a^k) \leq d/r < d$. Desta forma,

$$\{b \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \mathrm{ord}_p\, b = d\} \subset \{\overline{a}^k \mid 0 \leq k < d \text{ e } \mathrm{mdc}(k,d) = 1\},$$

portanto $N(d) \leq \varphi(d)$ (na verdade, os dois conjuntos acima são iguais, como ficará claro a partir da demonstração da proposição abaixo). □

Proposição 20. *Se p é um primo, então existe uma raiz primitiva módulo p.*

Demonstração. Para cada $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$, tem-se $\mathrm{ord}_p\, a \mid p-1$ e portanto $p-1 = \sum_{d|p-1} N(d)$. Por outro lado, temos pelos dois lemas acima que

$$p - 1 = \sum_{d|p-1} N(d) \leq \sum_{d|p-1} \varphi(d) = p - 1.$$

Logo devemos ter $N(d) = \varphi(d)$ para todo d. Em particular, $N(p-1) = \varphi(p-1) > 0$, logo existem raízes primitivas módulo p. □

Corolário 21. *Seja p um primo. Para cada $d \mid p-1$, existem exatamente $\varphi(d)$ elementos em $(\mathbb{Z}/p\mathbb{Z})^\times$ com ordem d. Em particular, p possui exatamente $\varphi(p-1)$ raízes primitivas.*

Com isto, encerramos a demonstração do teorema 12. Vejamos algumas aplicações.

Exemplo 22. *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 $m_k = 2^k r_k$, $r_k \in \mathbb{N}$. Se r_k é par, tome $m_{k+1} = 2\times 10^k + m_k = 2^{k+1}(5^k + r_k/2)$, e se r_k é ímpar, tome $m_{k+1} = 10^k + m_k = 2^{k+1}(5^k + r_k)/2$.

Como $m_{1000} \equiv 2 \pmod{10}$, 5 não divide $r_{1000} = \frac{m_{1000}}{2^{1000}}$. Portanto, como 2 é raiz primitiva módulo 5^{1000} pela proposição 16, existe $k \in \mathbb{N}$ com $2^k \equiv r_{1000} \pmod{5^{1000}}$. Logo $2^k = b5^{1000} + r_{1000}$ para algum $b \in \mathbb{N}$ e assim

$$2^{k+1000} = b10^{1000} + 2^{1000} r_{1000} = b10^{1000} + m_{1000},$$

e as 1000 últimas casas de 2^{k+1000} são as 1000 casas de m_{1000}, que pertencem todas a $\{1,2\}$. □

Observação 23. *Um grupo G é chamado de* cíclico *se existe um elemento g tal que $G = \{g^n \mid n \in \mathbb{Z}\}$. O fato de p^n e $2p^n$, p primo ímpar, admitirem raízes primitivas equivale a dizer que os grupos $(\mathbb{Z}/p^n\mathbb{Z})^\times$ e $(\mathbb{Z}/2p^n\mathbb{Z})^\times$ são cíclicos, ou ainda que há isomorfismos de grupos $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(p^n)$ e $(\mathbb{Z}/2p^n\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(2p^n)$ onde a operação nos grupos da direita é a adição.*

O leitor não deve ter dificuldades para adaptar a prova acima a fim de mostrar que todo corpo K com um número finito de elementos admite raiz primitiva, isto é, o seu grupo de unidades $K^\times = K \setminus \{0\}$ é um grupo cíclico.

Problemas Propostos

Problema 24. *Encontrar as ordens de* 2 *e* 5 *módulo* 101*. Encontrar também todos os elementos de ordem* 20 *em* $(\mathbb{Z}/101\mathbb{Z})^\times$*.*

Problema 25. *Determine um elemento de* $(\mathbb{Z}/99\mathbb{Z})^\times$ *de ordem* 30*.*

Problema 26. *Determine todos os valores de* n *para os quais* $|(\mathbb{Z}/n\mathbb{Z})^\times| = 24$*.*

Problema 27. *Determine um gerador de* $(\mathbb{Z}/242\mathbb{Z})^\times$*.*

Problema 28. *Demonstrar que* $2n \mid \varphi(a^n + 1)$ *para todo inteiro positivo* a*.*

Problema 29 (IMO1978)**.** *Sejam* m *e* n *inteiros positivos com* $m < n$*. Se os três últimos algarismos de* 1978^m *são os mesmos que os três últimos algarismos de* 1978^n*, encontrar* m *e* n *tais que* $m + n$ *assume o menor valor possível.*

Problema 30. *Sejam* d *e* n *números naturais tais que* $d \mid 2^{2^n} + 1$*. Demonstre que existe um inteiro* k *tal que* $d = k2^{n+1} + 1$*.*

Problema 31. *Seja* $k \geq 2$ *e* $n_1, n_2, \ldots, n_k \geq 1$ *números naturais que tem a propriedade*

$$n_2 \mid (2^{n_1} - 1), \quad n_3 \mid (2^{n_2} - 1), \ldots, n_k \mid (2^{n_{k-1}} - 1) \text{ e } n_1 \mid (2^{n_k} - 1)$$

Demonstrar que $n_1 = n_2 = \cdots = n_k = 1$*.*

Problema 32. *Mostrar que* $x^3 - x + \overline{1}$ *é irredutível em* $\mathbb{Z}/3\mathbb{Z}[x]$*. Encontrar todas as raízes primitivas do corpo finito* $\frac{\mathbb{Z}/3\mathbb{Z}[x]}{(x^3 - x + \overline{1})}$*.*

Problema 33 (Teorema de Lagrange)**.** *Seja* G *um grupo com número finito de elementos. Seja* H *um* subgrupo *de* G*, i.e., um subconjunto de* G *tal que* $a, b \in H \implies a \cdot b \in H$ *e* $a \in H \implies a^{-1} \in H$*, de modo que o produto de* G *se restringe a* H *e faz de* H *um grupo também.*

(a) Mostre que os subconjuntos de G *do tipo*

$$g \cdot H \stackrel{\text{def}}{=} \{g \cdot h \mid h \in H\}$$

formam uma partição de G*, ou seja, todo elemento de* G *pertence a algum* $g \cdot H$ *e que se* $g_1 \cdot H \cap g_2 \cdot H \neq \emptyset$*, então* $g_1 \cdot H = g_2 \cdot H$*.*

(b) Mostre que $|g_1 \cdot H| = |g_2 \cdot H|$ *para quaisquer* $g_1, g_2 \in G$ *e que portanto* $|H|$ *divide* $|G|$ *(teorema de Lagrange).*

(c) Seja $g \in G$*. Mostre que existe* $t > 0$ *tal que* $g^t = e$*. Se* $\operatorname{ord} g$ *é o menor* t *positivo com esta propriedade, mostre que*

$$H = \{g^n \mid n \in \mathbb{N}\}$$

é um subgrupo de G *com* $\operatorname{ord} g$ *elementos.*

(d) Aplicando o teorema de Lagrange ao subgrupo do item anterior, prove que $g^{|G|} = e$ *para todo* $g \in G$. *Observe que isto fornece uma nova prova do teorema de Euler-Fermat no caso em que* $G = (\mathbb{Z}/(n))^{\times}$.

Problema 34 (APMO1997). *Encontrar um* n *no conjunto* $\{100, 101, \ldots 1997\}$ *tal que* n *divide* $2^n + 2$.

Problema 35. *Definimos a* função de Carmichael $\lambda\colon \mathbb{N} \to \mathbb{N}$ *como o menor inteiro positivo tal que* $a^{\lambda(n)} \equiv 1 \pmod{n}$ *para todo* a *primo com* n. *Observe que, pelo teorema 12,* $\lambda(p^l) = p^{l-1}(p-1)$ *para todo* p *primo ímpar. Mostrar que*

(a) $\lambda(2) = 1$, $\lambda(4) = 2$ *e* $\lambda(2^l) = 2^{l-2}$ *para todo* $l \geq 3$.

(b) Se $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ *é a fatoração em primos de* n, *então*

$$\lambda(n) = \text{mmc}\{\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k})\}.$$

Problema 36 (IMO2000). *Existe um inteiro* N *divisível por exatamente* 2000 *primos diferentes e tal que* N *divide* $2^N + 1$*?*

Problema 37 (IMO1990). *Encontrar todos os números naturais* n *tais que* $n^2 \mid 2^n + 1$.

Problema 38 (IMO1999). *Encontrar todos os pares* (n, p) *de inteiros positivos tais que* p *é primo,* $n \leq 2p$ *e* $(p-1)^n + 1$ *é divisível por* n^{p-1}.

Problema 39 (Banco-IMO2000). *Determine todas as triplas* (a, m, n) *de inteiros positivos tais que* $a^m + 1 \mid (a+1)^n$.

Dicas e Soluções

Em breve

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.