Ano 2015

UMA RAIZ PRIMITIVA PARA AS RAÍZES N-ÉSIMAS DA UNIDADE

Oswaldo Rio Branco de Oliveira

http://www.ime.usp.br/~oliveira oliveira@ime.usp.br

Fixemos n em $\{1, 2, \ldots\}$. Pelo TFA a equação $z^n = 1$, tem n soluções em $\mathbb{C}$, ditas raízes n-ésimas da unidade. Denotemos por w uma arbitrária raiz n-ésima da unidade. Dada w, temos

$$\begin{cases} z^n - 1 = z^n - w^n = (z-w)Q(z), \text{ com } Q(z) = \sum_{j=0}^{n-1} z^{n-1-j}w^j \text{ um polinômio e} \\ Q(w) = nw^{n-1} \neq 0, \end{cases}$$

e portanto w é um zero simples do polinômio $z^n - 1$, com z em $\mathbb{C}$. Logo, existem n distintas raízes n-ésimas da unidade.

Dado k arbitrário em $\mathbb{N}^*$, um cálculo simples mostra que $\overline{w} = w^{-1}$ e w^k são raízes n-ésimas da unidade. Ainda mais,

$$|w^{k+1} - w^k| = |w^k(w-1)| = |w-1|.$$

Se w é real ou imaginário puro, então w pertence a $\{1, -1, i, -i\}$.

Dizemos que w é uma raiz primitiva das raízes n-ésimas da unidade se

$$w, w^2, \ldots, w^n \quad (\text{obviamente } w^n = 1)$$

são todas as n raízes n-ésimas da unidade.

Para provar a existência de uma raiz primitiva para as raízes n-ésimas da unidade, podemos supor n par. Pois, se w é uma raiz primitiva para as raízes $2n$-ésimas da unidade então $w^2, \ldots, w^{2n}$ são todas as n soluções distintas de $z^n = 1$. Melhor ainda, os casos $n = 2$ e $n = 4$ são triviais e podemos também supor $n \geq 6$.

Dado n par e $n \geq 6$, a equação $z^n = 1$ tem uma solução w não real e não imaginária pura. Também $\pm w$ e $\pm\overline{w}$ são soluções de $z^n = 1$. Portanto, existe uma raiz n-ésima da unidade com partes real e imaginária estritamente positivas.

Desta forma, existe uma raiz n-ésima da unidade na forma

$$\begin{cases} \zeta = \zeta(n) = a + ib, \text{ com } 0 < a < 1 \text{ e } 0 < b < 1, \\ \text{satisfazendo } 0 < |\zeta - 1| = r, \text{ onde } r = \min\{|w-1| : \ w^n = 1 \text{ e } \mathrm{Im}(w) > 0\}. \end{cases}$$

Destacamos que ζ satisfaz $r^2 = |\zeta - 1|^2 = (a-1)^2 + b^2 = 2 - 2a$. Ainda mais, ζ é a única raiz n-ésima da unidade satisfazendo $|\zeta - 1| = r$ e $\mathrm{Im}(\zeta) > 0$.

No que segue, consideramos um inteiro par $n \geq 6$ e mantemos a notação acima.

Lema 1. *Dado x em $[-1,1]$, seja $z_x = x + i\sqrt{1-x^2}$. Vale o que segue.*

(A) A função

$$\varphi : [-a,1] \to [-1,a], \text{ onde } \varphi(x) = Re(\zeta z_x) = ax - b\sqrt{1-x^2} \text{ se } x \in [-a,1],$$

é bijetora e estritamente crescente. Sua inversa é

$$\psi : [-1,a] \to [-a,1], \text{ onde } \psi(y) = Re(\zeta^{-1} z_y) = ay + b\sqrt{1-y^2} \text{ se } y \in [-1,a].$$

(B) Para $x \in [-1,-a] \cup [a,1]$, temos $(z_x)^n = 1$ se e somente se $x \in \{\pm 1, \pm a\}$.

Prova. Inicialmente, vejamos que φ e ψ estão bem definidas.

Dado x em $[-a,1]$, é bem trivial ver que $-1 \leq \mathrm{Re}(\zeta z_x) = ax - b\sqrt{1-x^2} \leq a$. Analogamente, dado y em $[-1,a]$ temos $-a \leq ay \leq ay + b\sqrt{1-y^2} = \mathrm{Re}(\zeta^{-1} z_y) \leq 1$.

(A) Se y está em $[-1,a]$, então $\mathrm{Im}(\zeta^{-1} z_y) = a\sqrt{1-y^2} - by$ é positivo em $[-1,0]$ e também em $[0,a]$ (pois decresce de a até 0 ao longo de $[0,a]$). Logo, $x = \mathrm{Re}(\zeta^{-1} z_y)$ satisfaz $z_x = \zeta^{-1} z_y$ e então segue $\varphi(x) = \mathrm{Re}(\zeta z_x) = y$.

Se x está em $[-a,1]$, então $\mathrm{Im}(\zeta z_x) = a\sqrt{1-x^2} + bx$ é positivo em $[-a,0]$ (crescendo de 0 até a) e em $[0,1]$. Portanto, $y = \mathrm{Re}(\zeta z_x)$ satisfaz

$$z_y = \zeta z_x. \tag{1.1}$$

Donde, $\psi(y) = \mathrm{Re}(\zeta^{-1} z_y) = x$.

Evidentemente, φ restrita a $[0,1]$ e ψ restrita a $[-1,0]$ são crescentes, com $\psi([-1,0]) = [-a,b]$. Portanto, $\varphi = \psi^{-1}$ restrita a $[-a,b]$ é crescente. Sendo assim, a bijeção φ é estritamente crescente em $[-a,1]$.

(B) Se x está em $(a,1)$, então temos $|z_x - 1|^2 = 2 - 2x < 2 - 2a = r^2$. Assim, pela definição de r, obtemos $(z_x)^n \neq 1$. Se $x \in \{a,1\}$, é óbvio que $(z_x)^n = 1$.

Como n é par, para x em $[-1,-a]$ e $z_x = x + i\sqrt{1-x^2}$, é suficiente aplicarmos o último páragrafo a $-x$ e $-x + i\sqrt{1-x^2} = -\overline{z_x}$ ♣

Teorema 2. *$\zeta = \zeta(n)$ é uma raiz primitiva das raízes n-ésimas da unidade.*
Prova.

Definamos por iteração a sequência $x_k = \varphi(x_{k-1})$, com $x_0 = 1$ e $k \geq 1$ tal que x_{k-1} está em $[-a, 1]$, o domínio de φ. A fórmula (1.1) mostra que $z_{x_k} = \zeta z_{x_{k-1}}$, com $z_{x_0} = 1 = \zeta^0$. Logo, por iteração, $z_{x_k} = \zeta^k$. Pelo Lema 1(A), a função φ é estritamente crescente e $x_2 = \varphi(x_1) < x_1 = \varphi(x_0) = a < x_0$. Então, por iteração, obtemos $x_k = \mathrm{Re}(\zeta^k) < x_{k-1} < \cdots < x_0 = 1$.

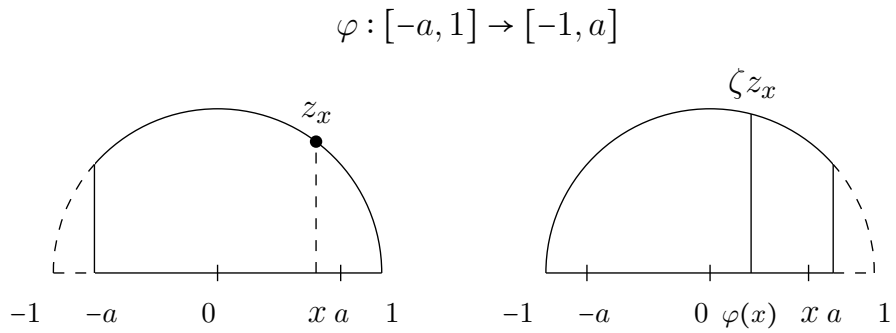

Figura 1: Uma raiz primitiva para $z^n = 1$.

Como há n n-ésimas raízes da unidade, existe o maior p em $\mathbb{N}$ satisfazendo

$$-1 \leq x_p < x_{p-1} < \cdots < x_2 < x_1 < x_0 = 1.$$

Dado $k = 2, \ldots, p$, a função φ é uma bijeção de $[x_{k-1}, x_{k-2}]$ sobre $[x_k, x_{k-1}]$. Logo, por indução em k, a fórmula (1.1) e o Lema 1(B), existem apenas dois valores de x em $[x_k, x_{k-1}]$ tais que $(z_x)^n = 1$. A saber, $x = x_k$ e $x = x_{k-1}$.

- ⋄ Mostremos $x_p = -1$. Se x_p está no domínio de φ, definindo $x_{p+1} = \varphi(x_p)$ obtemos $x_{p+1} = \varphi(x_p) < \varphi(x_{p-1}) = x_p$, contra a definição de p. Portanto, x_p está em $[-1, -a)$. Pelo Lema 1(B) obtemos $x_p = -1$ (e $\zeta^p = -1$).

Os subintervalos $[x_k, x_{k-1})$, com $k = 1, \ldots, p$, formam uma partição de $[-1, 1)$ e a cada subintervalo corresponde apenas uma raiz n-ésima da unidade no hemisfério superior $\{z \in \mathbb{C} : |z| = 1 \text{ e } \mathrm{Im}(z) \geq 0\}$. Assim, $\zeta^0, \zeta, \ldots, \zeta^p$ são todas as raízes n-ésimas da unidade no hemisfério superior e $\zeta^0, \ldots, , \zeta^p, \overline{\zeta}, \ldots, \overline{\zeta^{p-1}}$ são todas as n raízes n-ésimas da unidade. Logo, $n = 2p$. Para completar, dado k temos $\overline{\zeta^{p-k}} = \zeta^{-(p-k)} = \zeta^{2p}\zeta^{-p+k} = \zeta^{p+k}$ e então $\{\overline{\zeta^{p-1}}, \ldots, \overline{\zeta}\} = \{\zeta^{p+1}, \ldots, \zeta^{2p-1}\}$ ♣

Comentários.

- O Lema 1.1(A) pode ser provado de forma breve (e obscura), via derivação. A função $\varphi : [-a, 1] \to [-1, a]$ é contínua, satisfaz $\varphi(-a) = -1$ e $\varphi(1) = a$, e

$$\varphi'(x) = a + \frac{bx}{\sqrt{1-x^2}} = \frac{a\sqrt{1-x^2} + bx}{\sqrt{1-x^2}}, \text{ para todo } x \text{ em } (-a, 1).$$

  Então, dado x em $[0, 1)$, temos $\varphi'(x) \geq a > 0$. Se $-a < x < 0$, temos

$$\sqrt{1-x^2} > \sqrt{1-a^2} = b \quad \text{e} \quad a\sqrt{1-x^2} + bx > ab - ab = 0.$$

  Donde, φ é estritamente crescente e, pelo teorema do valor-intermediário, sua imagem é $[-1, a]$.

- Se n é primo e $w \neq 1$ é uma raiz n-ésima da unidade, uma argumentação simples mostra que w é uma raiz primitiva das raízes n-ésimas da unidade.

- Dado m em $\mathbb{N}^*$ e ζ, uma raiz primitiva das raízes n-ésimas da unidade, é trivial ver que

$$\zeta^m \text{ é uma raiz primitiva de tais raízes se e só se } \mathrm{mdc}(m, n) = 1.$$

- Seja ζ uma raiz primitiva das raízes n-ésimas da unidade. Então, dado um número c in $\mathbb{C}$, com $c \neq 0$, e z, uma raiz n-ésima arbitrária de c, é imediato provar que

$$\zeta^0 z, \zeta^1 z, \ldots, \zeta^{n-1} z$$

  são todas as n distintas raízes n-ésimas de c.

- Usando a função exponencial complexa, é fácil ver que

$$e^{i\frac{2\pi}{n}} \text{ é uma raiz primitiva das raízes } n\text{-ésimas da unidade.}$$

  Um cálculo trivial mostra

$$e^{i\frac{2\pi}{n}} = \zeta.$$

Departamento de Matemática
Universidade de São Paulo
São Paulo, SP - Brasil