# Material extra à Aula 3

Uma aplicação dos números complexos à combinatória: o filtro de raízes da unidade

**Aviso.** Estas notas foram geradas por inteligência artificial a partir do conteúdo apresentado em sala e da bibliografia do curso. Podem conter erros ou imprecisões; em caso de dúvida, consulte o livro-texto indicado no plano de ensino.

Estas notas complementam a segunda metade da Aula 3 e desenvolvem, com detalhes, a aplicação que discutimos em sala — inclusive as partes que não deu tempo de ver. Elas não usam nada além do que foi visto na primeira metade daquela aula: a forma polar e as raízes $n$-ésimas da unidade. A ideia central é que as raízes da unidade funcionam como um *detector de divisibilidade*, e que isso transforma problemas de contagem com restrições de congruência em contas com números complexos.

Os Apêndices A e B, que não foram vistos em sala e podem ser lidos independentemente do resto, trazem outras duas aplicações, de sabor mais geométrico: os polígonos regulares com vértices inteiros e o teorema de ladrilhamento de de Bruijn.

## 1 O lema: raízes da unidade detectam divisibilidade

**Lema 1.1.** *Sejam $m \geq 1$ inteiro e $\omega = \operatorname{cis}\frac{2\pi}{m}$. Para todo $k \in \mathbb{Z}$,*

$$\frac{1}{m}\sum_{j=0}^{m-1}\omega^{jk} = \begin{cases} 1, & \text{se } m \mid k, \\ 0, & \text{caso contrário.} \end{cases}$$

*Demonstração.* Se $m \mid k$, então $\omega^k = 1$ e cada uma das $m$ parcelas vale 1, de modo que a média vale 1. Se $m \nmid k$, então $\omega^k \neq 1$ e a soma geométrica dá

$$\sum_{j=0}^{m-1}\left(\omega^k\right)^j = \frac{\omega^{km}-1}{\omega^k-1} = \frac{1-1}{\omega^k-1} = 0,$$

pois $\omega^m = 1$. □

**Comentário.** No caso $k = 1$ o lema diz que a soma das $m$ raízes $m$-ésimas da unidade é zero: os vértices de um polígono regular inscrito no círculo unitário têm baricentro na origem. Vale desenhar a figura antes de escrever a conta — o que faremos a seguir é usar esse cancelamento perfeito como uma *peneira*.

## 2 O problema

Quantos subconjuntos de $\{1, 2, \ldots, n\}$ têm cardinalidade divisível por 3?

A resposta é a soma $\displaystyle\sum_{3\mid k}\binom{n}{k} = \binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \cdots$, para a qual não há fórmula

fechada evidente: o binômio de Newton sabe somar *todos* os $\binom{n}{k}$, mas não sabe selecionar alguns deles. É exatamente essa seleção que o Lema 1.1 fornece.

## 3 A conta

Seja $\omega = \operatorname{cis}\frac{2\pi}{3}$. Inserindo o filtro e trocando a ordem das somas:

$$\sum_{3|k}\binom{n}{k} = \sum_{k=0}^{n}\binom{n}{k}\cdot\frac{1}{3}\sum_{j=0}^{2}\omega^{jk} = \frac{1}{3}\sum_{j=0}^{2}\sum_{k=0}^{n}\binom{n}{k}\left(\omega^{j}\right)^{k} = \frac{1}{3}\sum_{j=0}^{2}\left(1+\omega^{j}\right)^{n}.$$

O passo decisivo é o último: para cada $j$ fixo, a soma interna é o binômio de Newton aplicado ao número complexo $\omega^j$.

Resta calcular $1+\omega$ na forma polar. Como $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$,

$$1+\omega = \frac{1}{2} + \frac{\sqrt{3}}{2}\,i = \operatorname{cis}\frac{\pi}{3},$$

que tem módulo 1. Vale a pena exibir isso geometricamente: somando os vetores 1 e $\omega$ pela regra do paralelogramo, o resultado cai de volta sobre o círculo unitário. Analogamente $1+\omega^2 = \overline{1+\omega} = \operatorname{cis}(-\frac{\pi}{3})$, e como $1+\omega^0 = 2$ obtemos

**Proposição 3.1.** *Para todo $n \geq 0$,*

$$\sum_{3|k}\binom{n}{k} = \frac{2^n + \operatorname{cis}\frac{n\pi}{3} + \operatorname{cis}(-\frac{n\pi}{3})}{3} = \frac{2^n + 2\cos\dfrac{n\pi}{3}}{3}.$$

**Verificação rápida.** Para $n=3$: $(8+2\cos\pi)/3 = (8-2)/3 = 2$, e de fato $\binom{3}{0}+\binom{3}{3} = 1+1 = 2$.

**A moral.** A resposta é *quase* $2^n/3$ — como se cada subconjunto tivesse "um terço de chance" de ter cardinalidade divisível por 3 —, e o desvio é um termo oscilante $2\cos(n\pi/3)$, de módulo no máximo 2 e periódico de período 6. A aritmética modular do problema aparece como *geometria no círculo unitário*: o erro é pequeno precisamente porque $|1+\omega| = 1$.

## 4 Fechamento: o caso divisível por 4

O mesmo argumento com $\omega = i$ dá

$$\sum_{4|k}\binom{n}{k} = \frac{2^n + (1+i)^n + 0^n + (1-i)^n}{4} = \frac{2^n + 2\operatorname{Re}\left((1+i)^n\right)}{4},$$

e agora $1+i=\sqrt{2}\,\operatorname{cis}\frac{\pi}{4}$, de módulo $\sqrt{2}>1$. Logo

$$\sum_{4\mid k}\binom{n}{k}=\frac{2^n+2^{\frac{n}{2}+1}\cos\dfrac{n\pi}{4}}{4}.$$

Confira com $n=4$: $(16+2^3\cos\pi)/4=(16-8)/4=2=\binom{4}{0}+\binom{4}{4}$.

Vale contrastar os dois casos: aqui o termo de erro *cresce* com $n$, mas com expoente $n/2$ em vez de $n$. Quem controla a ordem de grandeza da resposta é o *módulo* dos números $1+\omega^j$. Esse é um primeiro contato com uma ideia que retorna no estudo das séries de potências: o comportamento assintótico dos coeficientes é governado pela localização dos pontos relevantes no plano complexo.

## 5 Exercícios propostos

**Exercício 5.1.** Mostre que $\displaystyle\sum_{2\mid k}\binom{n}{k}=2^{n-1}$ para $n\geq 1$, primeiro pelo filtro com $\omega=-1$ e depois por uma bijeção entre subconjuntos de cardinalidade par e ímpar. Compare os dois argumentos.

**Exercício 5.2.** Fixe $m\geq 2$ e $0\leq r<m$. Mostre que

$$\sum_{k\equiv r\pmod m}\binom{n}{k}=\frac{1}{m}\sum_{j=0}^{m-1}\omega^{-jr}\big(1+\omega^j\big)^n,\qquad \omega=\operatorname{cis}\frac{2\pi}{m}.$$

Deduza, para $m=3$, o valor de $\sum_{k\equiv 1\ (3)}\binom{n}{k}$.

**Exercício 5.3.** Quantos subconjuntos de $\{1,2,\dots,n\}$ têm *soma* dos elementos divisível por 3? Sugestão: o número de subconjuntos com soma igual a $s$ é o coeficiente de $x^s$ em $\prod_{k=1}^{n}(1+x^k)$; aplique o filtro avaliando esse produto em $x=\omega^j$.

## Apêndice A Polígonos regulares com vértices inteiros

Esta é uma aplicação de sabor mais geométrico, que usa a multiplicação complexa como rotação. Identificamos $\mathbb{R}^2$ com $\mathbb{C}$ e o reticulado $\mathbb{Z}^2$ com o conjunto dos *inteiros de Gauss*

$$\mathbb{Z}[i]=\{a+bi:\ a,b\in\mathbb{Z}\},$$

que é fechado por soma, subtração e produto. Dizemos que um polígono é *inteiro* quando todos os seus vértices pertencem a $\mathbb{Z}[i]$.

**Teorema A.1.** *O único polígono regular inteiro é o quadrado. Mais precisamente, para $n\geq 3$ existe um polígono regular de $n$ lados com todos os vértices em $\mathbb{Z}^2$ se, e somente se, $n=4$.*

Que $n = 4$ ocorre é claro: $0,\ 1,\ 1+i,\ i$ são os vértices de um quadrado. A prova da recíproca se divide em dois argumentos independentes — um para $n = 3$ e $n = 6$, outro para os demais.

## A.1 O triângulo equilátero

**Lema A.2.** *Não existe triângulo equilátero inteiro.*

*Demonstração.* Suponha que $a, b, c \in \mathbb{Z}[i]$ sejam os vértices de um triângulo equilátero. Então $c$ é obtido de $b$ por uma rotação de $\pm 60°$ em torno de $a$, isto é,

$$c - a = (b - a)\ \mathrm{cis}(\pm\tfrac{\pi}{3}), \qquad \text{donde} \qquad \mathrm{cis}(\pm\tfrac{\pi}{3}) = \frac{c-a}{b-a}.$$

Escrevendo $u = c - a$ e $v = b - a$, ambos em $\mathbb{Z}[i]$ com $v \neq 0$, e racionalizando pelo conjugado,

$$\frac{u}{v} = \frac{u\bar{v}}{|v|^2}.$$

Aqui $u\bar{v} \in \mathbb{Z}[i]$ e $|v|^2$ é um inteiro positivo; logo $u/v$ tem parte real e parte imaginária *racionais*. Mas $\mathrm{cis}(\pm\frac{\pi}{3}) = \frac{1}{2} \pm \frac{\sqrt{3}}{2}i$ tem parte imaginária irracional, pois $\sqrt{3} \notin \mathbb{Q}$. Contradição. □

Isso resolve dois casos de uma vez:

- $n = 3$: é exatamente o lema;
- $n = 6$: se $a_0, a_1, \ldots, a_5$ é um hexágono regular inteiro, então os vértices alternados $a_0, a_2, a_4$ formam um triângulo equilátero, também inteiro — impossível.

*Observação* A.3. O mesmo cálculo dá uma prova alternativa do Teorema A.1 inteira: se $a_0, a_1, a_2$ são vértices consecutivos de um polígono regular inteiro de $n$ lados, então $\zeta = \mathrm{cis}\,\frac{2\pi}{n} = (a_2 - a_1)/(a_1 - a_0)$ tem, pelo argumento acima, parte real e imaginária racionais; ou seja, $\cos(2\pi/n)$ e $\mathrm{sen}(2\pi/n)$ são ambos racionais. Pelo teorema de Niven, os únicos valores racionais assumidos pelo cosseno de um múltiplo racional de $\pi$ são $0, \pm\frac{1}{2}, \pm 1$; destes, apenas $\cos(2\pi/n) = 0$ deixa o seno racional, o que força $n = 4$. É mais rápido, mas depende de um resultado externo — por isso a demonstração abaixo, autocontida, é a que apresentamos.

## A.2 A descida infinita

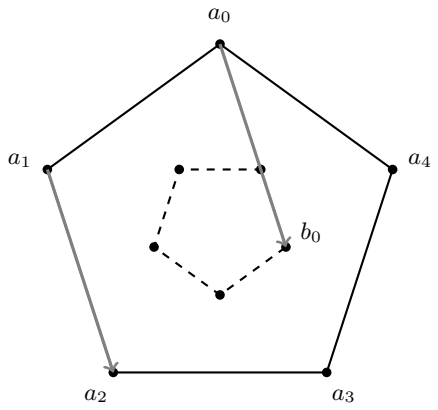
Trate agora $n \geq 5$ com $n \neq 6$. Sejam $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}[i]$ os vértices, em ordem cíclica, de um polígono regular de $n$ lados, e seja $c$ o seu centro. Como a rotação de ângulo $2\pi/n$ em torno de $c$ leva cada vértice no seguinte,

$$a_k = c + r\,\zeta^k, \qquad k = 0, 1, \ldots, n-1, \qquad \zeta = \mathrm{cis}\,\frac{2\pi}{n}, \quad r = a_0 - c \neq 0.$$

**A construção.** Defina (índices módulo $n$)

$$b_k = a_k + (a_{k+2} - a_{k+1}).$$

Geometricamente: transporte o vetor da aresta $a_{k+1}a_{k+2}$ para a ponta do vértice $a_k$. Como $\mathbb{Z}[i]$ é fechado por soma e subtração, cada $b_k$ é de novo um inteiro de Gauss.




**O cálculo.** Substituindo $a_k = c + r\zeta^k$,

$$b_k = c + r(\zeta^k + \zeta^{k+2} - \zeta^{k+1}) = c + r\zeta^k(1 - \zeta + \zeta^2) = c + r\zeta^k \cdot \zeta(\zeta^{-1} + \zeta - 1).$$

Como $\zeta^{-1} = \bar{\zeta}$ e $\zeta + \bar{\zeta} = 2\cos\theta$ com $\theta = 2\pi/n$, concluímos que

$$b_k = c + (r\lambda)\,\zeta^k, \qquad \lambda = \zeta(2\cos\theta - 1).$$

Ou seja: *os $b_k$ são os vértices de um polígono regular de $n$ lados, de mesmo centro $c$*, obtido do original por uma rotação seguida de uma homotetia de razão

$$|\lambda| = |2\cos\theta - 1|.$$

**A estimativa.** Para $n \geq 5$ temos $0 < \theta = 2\pi/n \leq 2\pi/5 < \pi/2$, logo $0 < \cos\theta < 1$ e portanto

$$-1 < 2\cos\theta - 1 < 1, \qquad \text{isto é,} \qquad |\lambda| < 1.$$

Além disso $\lambda = 0$ apenas se $\cos\theta = \frac{1}{2}$, ou seja $n = 6$ — caso já excluído. Assim $0 < |\lambda| < 1$: o novo polígono é não degenerado e *estritamente menor*.

**A contradição.** Iterando a construção $m$ vezes obtemos, para todo $m \geq 1$, um polígono regular inteiro de $n$ lados cujo raio é $|r|\,|\lambda|^m$ e cujo lado mede

$$\ell_m = 2\,|r|\,|\lambda|^m \operatorname{sen}\frac{\pi}{n} \xrightarrow[m\to\infty]{} 0.$$

Mas os vértices são pontos distintos de $\mathbb{Z}^2$, e dois pontos distintos de $\mathbb{Z}^2$ estão a distância pelo menos 1; logo $\ell_m \geq 1$ para todo $m$. Contradição. □

**Comentário.** A frase que resume tudo é: *um reticulado não admite escalas arbitrariamente pequenas.* A descida infinita é o análogo geométrico do argumento clássico para a irracionalidade de $\sqrt{2}$, e o papel dos complexos foi transformar a construção geométrica "transportar a aresta seguinte" na multiplicação por um único número $\lambda$, cujo módulo diz na hora se o polígono encolheu.

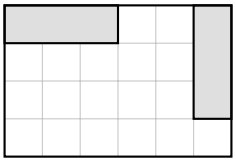
**Exercício A.4.** Verifique numericamente a razão $|\lambda| = |2\cos(2\pi/n) - 1|$ para $n = 5, 7, 8, 12$ e explique por que $|\lambda| \to 1$ quando $n \to \infty$. A descida fica mais lenta, mas ainda funciona — por quê?

**Exercício A.5.** Onde exatamente a demonstração de A.2 falha quando $n = 4$? Faça o desenho da construção $b_k = a_k + a_{k+2} - a_{k+1}$ para o quadrado $0, 1, 1+i, i$ e interprete o resultado.

## Apêndice B Ladrilhamento por peças $1 \times k$ (de Bruijn)

Aqui as raízes da unidade voltam no papel exato do Lema 1.1: pesos que somam zero. É uma *coloração com números complexos*, e substitui com vantagem os argumentos de coloração usuais.

**Teorema B.1** (de Bruijn)**.** *Sejam $k \geq 2$ e $m, n \geq 1$ inteiros. O retângulo $m \times n$ pode ser ladrilhado por peças $1 \times k$ (colocadas horizontal ou verticalmente, sem sobreposições e sem buracos) se, e somente se, $k \mid m$ ou $k \mid n$.*



Uma peça $1 \times 3$ horizontal e uma vertical dentro de um retângulo $6 \times 4$ (aqui $3 \mid 6$).

*Demonstração.* ($\Leftarrow$) Se $k \mid n$, cada uma das $m$ linhas $1 \times n$ se parte em $n/k$ peças horizontais; se $k \mid m$, procede-se por colunas.

($\Rightarrow$) Indexe as casas do retângulo por pares $(a, b)$ com $1 \leq a \leq m$ e $1 \leq b \leq n$, e atribua à casa $(a, b)$ o *peso complexo*

$$w(a, b) = \omega^{a+b}, \qquad \omega = \operatorname{cis} \frac{2\pi}{k}.$$

*Passo 1: cada peça tem peso total zero.* Uma peça horizontal ocupa as casas $(a, b), (a, b+1), \ldots, (a, b+k-1)$, e a soma dos seus pesos é

$$\sum_{j=0}^{k-1} \omega^{a+b+j} = \omega^{a+b} \sum_{j=0}^{k-1} \omega^j = 0,$$

pois $\sum_{j=0}^{k-1} \omega^j = 0$ pelo Lema 1.1 (é o caso em que $k \nmid 1$, válido porque $k \geq 2$). Uma peça vertical ocupa $(a, b), (a+1, b), \ldots, (a+k-1, b)$ e o cálculo é idêntico. *A orientação da*

*peça é irrelevante* — é exatamente por isso que o peso foi escolhido dependendo apenas da soma $a + b$.

*Passo 2: a soma total fatora.* Se o retângulo é ladrilhado, ele é a união disjunta das peças, e somando o Passo 1 sobre todas elas obtemos

$$0 = \sum_{a=1}^{m} \sum_{b=1}^{n} \omega^{a+b} = \left( \sum_{a=1}^{m} \omega^{a} \right) \left( \sum_{b=1}^{n} \omega^{b} \right).$$

*Passo 3: um dos fatores se anula.* Como $\mathbb{C}$ é um corpo, um produto nulo tem um fator nulo. Ora, $\omega \neq 1$ porque $k \geq 2$, e a soma geométrica dá

$$\sum_{a=1}^{m} \omega^{a} = \omega \, \frac{\omega^{m} - 1}{\omega - 1},$$

que se anula se, e somente se, $\omega^{m} = 1$, isto é, se e somente se $k \mid m$. Analogamente o segundo fator se anula exatamente quando $k \mid n$. Logo $k \mid m$ ou $k \mid n$. □

**Comentário.** Vale começar pelo caso concreto: *um tabuleiro* $10 \times 10$ *não pode ser ladrilhado por peças* $1 \times 4$, pois $4 \nmid 10$ — um fato nada evidente que a conta acima liquida em três linhas. Depois destacar os dois pontos em que os complexos fazem o trabalho: (i) o peso $\omega^{a+b}$ se fatora como $\omega^{a} \cdot \omega^{b}$, e é essa fatoração que separa as duas conclusões possíveis $k \mid m$ e $k \mid n$; (ii) a conclusão "um dos fatores é zero" usa que $\mathbb{C}$ não tem divisores de zero — a mesma estrutura de corpo discutida na primeira aula, agora fazendo trabalho combinatório de verdade.

**Exercício B.2.** Mostre que um tabuleiro $6 \times 6$ não pode ser ladrilhado por peças $1 \times 4$, e exiba um ladrilhamento de $8 \times 6$ por peças $1 \times 4$.

**Exercício B.3.** Generalize o Teorema B.1 para três dimensões: um bloco $a \times b \times c$ pode ser preenchido por barras $1 \times 1 \times k$ se, e somente se, $k$ divide $a$, $b$ ou $c$. Sugestão: use o peso $\omega^{x+y+z}$.

**Exercício B.4.** O que acontece se as peças $1 \times k$ forem substituídas por peças $1 \times k$ *apenas horizontais*? Enuncie e demonstre o critério correspondente.