

p -ágonos e Raízes da Unidade

Nesse breve artigo vamos discutir um problema utilizado no primeiro “pré-teste de seleção” do Irã em 2005. Na verdade, este é o problema A.27 da edição de novembro de 2001 da fantástica revista *Kömal*.

A princípio, um problema de Geometria, com um toque de teoria dos números, mas que no final das contas é resolvido utilizando conceitos de álgebra, em especial raízes p -ésimas da unidade. Quem resolveu o problema, no entanto, não fui eu; foi o Gabriel Bujokas. Digamos que eu sou o “porta-voz” dele nessa solução.

Para entender essa resolução desse problema você tem que ter certa familiaridade com raízes da unidade.

Problema. *Seja H_1 um polígono de p lados, sendo p primo. A seqüência de polígonos H_1, H_2, \dots, H_p é construída da seguinte maneira: dado o polígono H_k , H_{k+1} é obtido refletindo cada vértice de H_k em relação ao seu k -ésimo vértice vizinho, contando no sentido anti-horário. Prove que H_1 e H_p são polígonos semelhantes.*

Solução (por Gabriel Tavares Bujokas). A primeira parte do problema é bastante natural no seguinte aspecto: é natural pensar em vetores nesse ponto, já que os vértices são obtidos através de reflexões. Sendo assim, sejam $A_k^1, A_k^2, \dots, A_k^p$ os vértices de H_k , ordenados no sentido anti-horário. O vértice A_{k+1}^m de H_{k+1} é, então, obtido a partir da reflexão de A_k^m em relação ao seu k -ésimo vizinho A_k^{m+k} (é só somar k no índice relativo ao vértice; se $k+m$ ultrapassar p , tome o índice mód p). Logo A_k^{m+k} é o ponto médio de $A_k^m A_{k+1}^m$, ou seja,

$$A_k^{m+k} = \frac{A_k^m + A_{k+1}^m}{2} \iff A_{k+1}^m = 2A_k^{m+k} - A_k^m$$

Poderíamos pensar em resolver essa recorrência para encontrar os vértices de H_p , mas isso não parece ser simples considerando que a equação de recorrência obtida não é linear (por quê? veja que temos dois índices e que um depende do outro!).

Primeiro, vamos ajustar um pouco a equação para lados em vez de vértices. Seja $\ell_k^m = A_k^{m+1} - A_k^m$ o m -ésimo lado do polígono H_k (como vetor). Temos

$$\begin{cases} A_{k+1}^{m+1} = 2A_k^{m+1+k} - A_k^{m+1} \\ A_{k+1}^m = 2A_k^{m+k} - A_k^m \end{cases} \implies (A_{k+1}^{m+1} - A_{k+1}^m) = 2(A_k^{m+1+k} - A_k^{m+k}) - (A_k^{m+1} - A_k^m) \\ \iff \ell_{k+1}^m = 2\ell_k^{m+k} - \ell_k^m \quad (*)$$

Aí entra a principal idéia de Gabriel: como levar em consideração que p é primo? Ele resolveu considerar raízes da unidade. Seja $\zeta = e^{i\frac{2\pi}{p}}$ a raiz primitiva da unidade. A princípio, isso seria mais natural se algum dos p -ágonos fosse regular, de modo que fosse possível associar a cada vértice uma raiz p -ésima da unidade.

Mas a idéia genial de Gabriel foi considerar, para cada polígono, uma expressão: associe ao polígono H_k a expressão

$$h(k) = \ell_k^1 + \zeta \ell_k^2 + \zeta^2 \ell_k^3 + \dots + \zeta^{p-1} \ell_k^p = \sum_{m=1}^p \zeta^{m-1} \ell_k^m$$

O legal dessas expressões é que, por causa da relação de recorrência, podemos escrever $h(k+1)$ em

função de $h(k)$ de uma maneira bastante conveniente.

$$\begin{aligned}
h(k+1) &= \sum_{m=1}^p \zeta^{m-1} \ell_{k+1}^m = \sum_{m=1}^p \zeta^{m-1} (2\ell_k^{m+k} - \ell_k^m) \\
&= 2 \sum_{m=1}^p \zeta^{m-1} \ell_k^{m+k} - \sum_{m=1}^p \zeta^{m-1} \ell_k^m \\
&= 2\zeta^{-k} \sum_{m=1}^p \zeta^{m+k-1} \ell_k^{m+k} - \sum_{m=1}^p \zeta^{m-1} \ell_k^m \\
&= (2\zeta^{-k} - 1)h(k) \\
&= \left(\frac{2 - \zeta^k}{\zeta^k} \right) h(k)
\end{aligned}$$

Agora, escrever $h(p)$ em função de $h(1)$ é simples: aplicando essa última relação $p-1$ vezes, obtemos

$$h(p) = \left(\frac{2 - \zeta^{p-1}}{\zeta^{p-1}} \right) \left(\frac{2 - \zeta^{p-2}}{\zeta^{p-2}} \right) \cdots \left(\frac{2 - \zeta}{\zeta} \right) \left(\frac{2 - 1}{1} \right) h(1) = \frac{(2 - \zeta^{p-1})(2 - \zeta^{p-2}) \cdots (2 - 1)}{\zeta^{1+2+\cdots+(p-1)}} h(1)$$

Lembrando da fantástica fatoração

$$x^p - 1 = (x - 1)(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{p-1}),$$

e notando que $\zeta^{1+2+\cdots+(p-1)} = \zeta^{p \cdot \frac{p-1}{2}} = 1^{\frac{p-1}{2}} = 1$, obtemos a incrível relação

$$h(p) = (2^p - 1)h(1)$$

Isso é muito bom: se abrirmos $h(p)$ e $h(1)$, obtemos

$$\ell_p^1 + \zeta \ell_p^2 + \cdots + \zeta^{p-1} \ell_p^p = (2^p - 1)(\ell_1^1 + \zeta \ell_1^2 + \cdots + \zeta^{p-1} \ell_1^p)$$

Mas infelizmente a partir disso não podemos dizer (ainda) que $\ell_p^m = (2^p - 1)\ell_1^m$. Chegamos muito perto, mas precisamos de algo mais.

Para isso, usamos polinômios! Note que, a partir da relação (*), podemos concluir que cada ℓ_k^m é uma combinação linear racional dos lados $\ell_1^1, \ell_1^2, \dots, \ell_1^p$ de H_1 , ou seja, existem racionais a_1, a_2, \dots, a_p tais que

$$\ell_k^m = a_1 \ell_1^1 + a_2 \ell_1^2 + a_3 \ell_1^3 + \cdots + a_p \ell_1^p$$

Para não cairmos em complicações do tipo “todo vetor do plano é combinação linear de dois vetores”, associe a cada ℓ_1^m o monômio x^{m-1} e a cada ℓ_k^m o polinômio

$$P_k^m(x) = a_1 + a_2 x + a_3 x^2 + \cdots + a_p x^{p-1}$$

onde os a_m 's são os mesmos da outra equação. Vamos reescrever a equação de recorrência (*) em termos dessa nova associação. Ah, e o m em P_k^m não é expoente, é só uma notação. A recorrência fica

$$P_{k+1}^m(x) = 2P_k^{m+k}(x) - P_k^m(x)$$

Você pode provar por indução que, se q e r são inteiros e você associar x^{pq+r} a ℓ_1^r , $P_k^{m+k}(x) = x^k P_k^m(x)$. Então

$$P_{k+1}^m(x) = (2x^k - 1)P_k^m(x)$$

Logo, indutivamente, chegamos em

$$P_p^m(x) = (2x^{p-1} - 1)(2x^{p-2} - 1) \dots (2x - 1)P_1^m(x)$$

Mas ℓ_1^m está simplesmente associado a x^{m-1} , então

$$P_p^m(x) = (2x^{p-1} - 1)(2x^{p-2} - 1) \dots (2x - 1)x^{m-1}$$

Agora sim, as raízes da unidade entram em ação: faça $x = \zeta^t$, $t = 0, 1, 2, \dots, p - 1$. Obtemos, como na conta que fizemos com $h(p)$,

$$P_p^m(\zeta^t) = (2^p - 1)(\zeta^t)^{m-1}$$

Assim, se considerarmos

$$Q_p^m(x) = P_p^m(x) - (2^p - 1)x^{m-1}$$

vemos que ζ^t , $t = 0, 1, 2, \dots, p - 1$, é raiz de $Q_p^m(x)$. Isso quer dizer que esse polinômio é divisível por $(x - 1)(x - \zeta)(x - \zeta^2) \dots (x - \zeta^{p-1}) = x^p - 1$. Portanto, sendo $x^p - 1$ um polinômio mônico, existe um polinômio $G(x)$, de coeficientes inteiros, tal que

$$P_p^m(x) - (2^p - 1)x^{m-1} = G(x)(x^p - 1) \iff P_p^m = (2^p - 1)x^{m-1} + x^p G(x) - G(x)$$

Como $x^p G(x)$ e $G(x)$ representam a mesma combinação linear, já que x^{p+m} e x^m representam ambos ℓ_1^m , ao escrevermos ℓ_p^m como combinação linear de $\ell_1^1, \ell_1^2, \dots, \ell_1^p$, obtemos

$$\ell_p^m = (2^p - 1)\ell_1^m$$

Logo, como cada lado ℓ_p^m está no mesmo sentido e é proporcional ao lado ℓ_1^m , os polígonos H_p e H_1 são semelhantes. E a razão de semelhança é igual a $2^p - 1$! ■