XIX Semana Olímpica de Matemática

Nível 3

Polinômios em Z[x]

Matheus Secco

O projeto da XIX Semana Olímpica de Matemática foi patrocinado por:

impa
instituto nacional de matemática pura e aplicada

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

fundação lemann

Olimpíada Brasileira de Matemática

Polinômios em $\mathbb{Z}[x]$

N3 – Professor Matheus Secco

1 Ferramentas

Teorema 1 *(Forma Fatorada) Se $P(x)$ é um polinômio de grau n com raízes $r_1, r_2, \ldots, r_n$, podemos escrever*

$$P(x) = a(x - r_1)(x - r_2)\ldots(x - r_n),$$

onde a é uma constante.

Exemplo 1 *(Canadá 1970) Seja $P(x)$ um polinômio com coeficientes inteiros. Suponha que existam quatro inteiros distintos a, b, c, d tais que $P(a) = P(b) = P(c) = P(d) = 5$. Prove que não existe um inteiro k tal que $P(k) = 8$.*

Solução: Seja $Q(x) = P(x) - 5$. Logo, podemos escrever

$$Q(x) = (x - a)(x - b)(x - c)(x - d)R(x),$$

onde $R(x)$ é um polinômio com coeficientes inteiros. Se existe k tal que $P(k) = 8$, temos que $Q(k) = 3$ e, portanto,

$$(k - a)(k - b)(k - c)(k - d)R(k) = 3$$

Como 3 é primo, dentre $(k-a), (k-b), (k-c)$ e $(k-d)$, há pelo menos três deles iguais a 1 ou -1 e assim há pelo menos dois deles iguais. Supondo sem perdas que $k - a = k - b$, obtemos $a = b$, contradição. □

Teorema 2 *Se $P(x)$ é um polinômio com coeficientes inteiros e a e b são inteiros, então*

$$a - b \mid P(a) - P(b)$$

Demonstração: Seja $P(x) = a_n x^n + \cdots + a_1 x + a_0$. Logo $P(a) - P(b) = a_n(a^n - b^n) + \cdots + a_1(a - b)$. Pela fatoração $a^k - b^k = (a - b)\left(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}\right)$, temos que $a - b$ divide $a^k - b^k$ para todo $1 \leqslant k \leqslant n$ e, portanto, $a - b$ divide $P(a) - P(b)$. □

Exemplo 2 *(EUA 1974) Sejam a, b, c três inteiros distintos. Prove que não existe um polinômio $P(x)$ com coeficientes inteiros tal que $P(a) = b, P(b) = c$ e $P(c) = a$.*

Solução: Suponha por absurdo que existe tal polinômio. Sem perda de generalidade, suponha que $a = \max(a, b, c)$. Pelo **Teorema 2**,

$$a - b \mid P(a) - P(b) = b - c \quad \text{(i)}$$

$$a - c \mid P(a) - P(c) = b - a \text{ (ii)}$$

Se $b > c$, por (ii), $a - c \leqslant a - b \Leftrightarrow b \leqslant c$, absurdo.
Se $b < c$, por (i), $a - b \leqslant c - b \Leftrightarrow a \leqslant c$, absurdo. □

Teorema 3 *(Teorema das raízes racionais) Se* $P(x) = a_n x^n + \ldots + a_0$, $a_0 \neq 0$, *é um polinômio com coeficientes inteiros e* $\frac{p}{q}, \text{mdc}(p, q) = 1$, *é uma raiz racional de* P, *então* $p \mid a_0$ *e* $q \mid a_n$.

Exemplo 3 *(Teste IMO China 2005) Prove que o número*

$$\sqrt{1001^2 + 1} + \sqrt{1002^2 + 1} + \cdots + \sqrt{2000^2 + 1}$$

é irracional.

Solução: Considerando o polinômio P, mônico de grau 2^{1000}, cujas raízes são os números

$$\pm\sqrt{1001^2 + 1} \pm \sqrt{1002^2 + 1} \pm \cdots \pm \sqrt{2000^2 + 1},$$

temos que P possui coeficientes inteiros (tente provar isto!). Portanto, se

$$\sqrt{1001^2 + 1} + \sqrt{1002^2 + 1} + \cdots + \sqrt{2000^2 + 1}$$

é racional, pelo teorema das raízes racionais, deve ser um número inteiro. Provaremos então que

$$\sqrt{1001^2 + 1} + \sqrt{1002^2 + 1} + \cdots + \sqrt{2000^2 + 1}$$

não é inteiro.

Para isso, veja que

$$k < \sqrt{k^2 + 1} < k + \frac{1}{2k}.$$

Assim,

$$1001 + \cdots + 2000 < \sqrt{1001^2 + 1} + \sqrt{1002^2 + 1} + \cdots + \sqrt{2000^2 + 1} < 1001 + \frac{1}{2}\left(\frac{1}{1001} + \cdots + \frac{1}{2000}\right)$$

Desta maneira, basta provarmos que

$$S = \frac{1}{1001} + \cdots + \frac{1}{2000} < 2$$

Para isso, veja que $S < \frac{1000}{1001} < 2$, como queríamos. □

Teorema 4 *(Schur) Seja* P *um polinômio não constante com coeficientes inteiros. Então o conjunto dos números primos que dividem pelo menos um número não nulo do conjunto* $\{P(n) : n \in \mathbb{Z}\}$ *é infinito.*

Demonstração: Suponha que o conjunto dos primos que dividem algum número do conjunto dos números primos que dividem pelo menos um número não nulo do conjunto $\{P(n) : n \in \mathbb{Z}\}$ é finito. Considere agora o número n_0 tal que $P(n_0)$ tenha a maior quantidade de fatores primos, digamos j. Podemos escrever então $P(n_0) = \pm p_1^{\alpha_1} \ldots p_j^{\alpha_j} = k$. Considerando $Q(x) = P(x - n_0)$, podemos supor que $n_0 = 0$. Assim, teremos $P(x) = a_n x^n + \cdots + a_1 x + k$. Tomando $x = wk^2, w \in \mathbb{Z}$, temos que $P(wk^2) \equiv k (\text{mod } k^2)$. Logo podemos escrever $P(wk^2) = ak^2 + k = k(ak + 1)$. Como

$\mathrm{mdc}(k, ak+1) = 1$, se $ak+1 \neq \pm 1$, temos que $P(wk^2)$ terá um fator primo a mais que $P(n_0)$, o que é absurdo. De fato, isto deve acontecer, pois $P(x) = \pm k$ admite no máximo $2n$ raízes inteiras, enquanto $wk^2, w \in \mathbb{Z}$, pode assumir infinitos valores. □

Exemplo 4 *(Ibero Universtiária 2003) Prove que se $P(x)$ é um polinômio não constante com coeficientes inteiros, então existe n inteiro tal que $P(n)$ tem mais de 2003 fatores primos distintos.*

Solução: Pelo **Teorema de Schur**, existem primos distintos $p_1, \ldots, p_{2004}$ e inteiros distintos $x_1, \ldots, x_{2004}$ tais que $P(x_i)$ é divisível por p_i para $1 \leqslant i \leqslant 2004$. Pelo **Teorema Chinês dos Restos**, existe n inteiro tal que $n \equiv x_i \pmod{p_i}$ para $1 \leqslant i \leqslant 2004$. Pelo **Teorema 2**,

$$P(n) \equiv P(x_i) \equiv 0 \pmod{p_i},$$

o que mostra que $P(n)$ tem mais de 2003 fatores primos distintos. □

Teorema 5 *Um número α é dito **algébrico** se existe um polinômio mônico de coeficientes racionais possuindo α como raiz. Um tal polinômio de grau mínimo é único e é dito **polinômio minimal** de α. Todo polinômio com coeficientes racionais que possui α como raiz é divisível pelo polinômio minimal de α. Além disso, o polinômio minimal é irredutível em $\mathbb{Q}[x]$.*

Exemplo 5 *Seja $p(x)$ um polinômio irredutível em $\mathbb{Q}[x]$ de grau ímpar. Sejam $q(x), r(x) \in \mathbb{Q}[x]$ tais que $p(x)$ divide $q(x)^2 + q(x)r(x) + r(x)^2$. Prove que $p(x)^2$ divide $q(x)^2 + q(x)r(x) + r(x)^2$.*

Solução: Sem perda de generalidade, suponha que p é mônico. Como p tem grau ímpar, p possui uma raiz real, digamos α. Uma vez que p é irredutível, p deve ser o polinômio minimal de α. Por outro lado, se α é raiz de p, então $q(\alpha)^2 + q(\alpha)r(\alpha) + r(\alpha)^2 = 0$. Como α é real, devemos ter $q(\alpha) = r(\alpha) = 0$ e, portanto, α é raiz de q e r. Logo q e r são divisíveis por p e então $p(x)^2$ divide $q(x)^2 + q(x)r(x) + r(x)^2$. □

2 Problemas

Problema 1 (OBM-U 1 fase 2013) Seja $P(x)$ um polinômio com coeficientes inteiros satisfazendo $P(n) = n$ para todo n inteiro com $1 \leqslant n \leqslant 6$ e $|P(0)| \leqslant 2013$. Determine quantos e quais são os possíveis valores de $P(0)$.

Problema 2 (Rússia 2004) Seja $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$ um polinômio com coeficientes inteiros não nulos que possui n raízes inteiras distintas duas a duas. Prove que se as raízes são duas a duas primas entre si, então a_{n-1} e a_n são primos entre si.

Problema 3 (IMO 1974) Seja $P(x)$ um polinômio com coeficientes inteiros. Seja $\deg(P) \geqslant 1$ o grau de P. Seja $n(P)$ o número de inteiros k para os quais $[P(k)]^2 = 1$. Prove que $n(P) - \deg(P) \leqslant 2$.

Problema 4 (Banco IMO 1982) Seja $p(x)$ um polinômio mônico de grau 3 com coeficientes inteiros tal que uma de suas raízes é igual ao produto das outras duas. Prove que $2p(-1)$ é múltiplo de $p(1) + p(-1) - 2(1 + p(0))$.

Problema 5 (Banco IMO 1989) Prove que para todo $n > 1$ inteiro positivo a equação

$$\sum_{k=1}^{n} \frac{x^k}{k!} = -1$$

não possui raízes racionais.

Problema 6 (Balcânica 1994) Seja n um inteiro. Prove que o polinômio

$$f(x) = x^4 - 1994x^3 + (1993 + n)x^2 - 11x + n$$

possui no máximo uma raiz inteira.

Problema 7 (Centroamericana 2013) Determine todos os pares de polinômios não constantes $p(x)$ e $q(x)$ mônicos de grau n, que possuam n raízes inteiras não negativas e tais que $p(x) - q(x) = 1$.

Problema 8 (Baltic Way 1994) Seja $p(x)$ um polinômio com coeficientes inteiros tal que as equações $p(x) = 1$ e $p(x) = 3$ possuem soluções inteiras. É possível que a equação $p(x) = 2$ tenha duas soluções inteiras distintas?

Problema 9 (Baltic Way 2013) Sejam k e n inteiros positivos e sejam $x_1, x_2, \cdots, x_k, y_1, y_2, \cdots, y_n$ inteiros distintos dois a dois. Um polinômio P com coeficientes inteiros satisfaz

$$P(x_1) = P(x_2) = \cdots = P(x_k) = 54$$

$$P(y_1) = P(y_2) = \cdots = P(y_n) = 2013.$$

Determine o valor máximo de n.

Problema 10 (Zhautykov 2014) Existe polinômio $P(x)$ com coeficientes inteiros tal que $P(1+\sqrt{3}) = 2 + \sqrt{3}$ e $P(3 + \sqrt{5}) = 3 + \sqrt{5}$.

Problema 11 (Torneio das Cidades 05) No gráfico de um polinômio com coeficientes inteiros, há dois pontos que possuem coordenadas inteiras. Prove que se a distância entre esses dois pontos também é inteira, então o segmento que os une é paralelo ao eixo das abscissas.

Problema 12 (Banco IMO 2005) Sejam a, b, c, d, e, f inteiros positivos. Suponha que $S = a + b + c + d + e + f$ divida $abc + def$ e $ab + bc + ca - de - ef - fd$. Prove que S é composto.

Problema 13 (Putnam 2000) Seja $f(x)$ um polinômio com coeficientes inteiros. Defina uma sequência $a_0, a_1, \cdots$ de inteiros de forma que $a_0 = 0$ e $a_{n+1} = f(a_n)$ para todo $n \geqslant 0$. Prove que se existe um inteiro positivo m para o qual $a_m = 0$, então $a_1 = 0$ ou $a_2 = 0$.

Problema 14 (IMO 2006) Seja $P(x)$ um polinômio de grau $n > 1$ com coeficientes inteiros e seja k um inteiro positivo. Considere o polinômio $Q(x) = P(P(\ldots P(P(x))\ldots))$, onde P aparece k vezes. Prove que existem no máximo n inteiros t tais que $Q(t) = t$.

Problema 15 (Irã 2004) Seja $P(x)$ um polinômio com coeficientes inteiros tal que $P(n) > n$ para todo inteiro positivo n. Defina uma sequência x_k da seguinte forma: $x_1 = 1$, $x_{i+1} = P(x_i)$ para $i \geqslant 1$. Para cada inteiro positivo m, existe um termo em tal sequência divisível por m. Prove que $P(x) = x + 1$.

Problema 16 (APMO 2001) Um ponto no plano cartesiano é dito **misto** se uma de suas coordenadas é racional e a outra é irracional. Encontre todos os polinômios com coeficientes reais tais que seus gráficos não contêm pontos mistos.

Problema 17 (Teste Romênia 1997) Sejam $P(x), Q(x)$ polinômios mônicos, irredutíveis e com coeficientes racionais. Suponha que a e b são tais que $P(a) = Q(b) = 0$ e $a + b$ é racional. Prove que $P(x)^2 - Q(x)^2$ possui uma raiz racional.

Problema 18 (OBM-U 2006) Seja p um polinômio irredutível em $\mathbb{Q}[x]$ de coeficientes racionais e grau maior do que 1. Prove que se p admite duas raízes r e s cujo produto é 1, então o grau de p é par.

Problema 19 (Teste IMO EUA 2005) Um polinômio $f(x)$ com coeficientes inteiros é dito especial se para qualquer inteiro positivo $k > 1$, a sequência $f(1), f(2), f(3), \cdots$ possui algum número que é primo entre si com k. Seja n um inteiro maior do que 1. Escolhe-se aleatoriamente um polinômio mônico de grau n com coeficientes em $\{1, 2, 3, \cdots, n!\}$. Prove que a probabilidade de este polinômio ser especial está entre 71% e 75% .

Problema 20 (Banco IMO 2011) Sejam $P(x)$ e $Q(x)$ dois polinômios com coeficientes inteiros tais que não há polinômio não constante com coeficientes racionais que divida $P(x)$ e $Q(x)$. Suponha que, para todo n inteiro positivo, os inteiros $P(n)$ e $Q(n)$ são positivos e que $2^{Q(n)} - 1$ divide $3^{P(n)} - 1$. Prove que $Q(x)$ é constante.