Polinômios com Teoria dos Números

Sofia Pinheiro

1 Introdução

Os polinômios são expressões algébricas formadas por termos com coeficientes e variáveis elevadas a expoentes naturais. Eles são essenciais em várias áreas da matemática e suas propriedades permitem resolver equações e modelar fenômenos. Neste trabalho, exploraremos suas operações, fatoração e aplicações.

2 Analizar valores

Comecemos, então, pelo mais simples: **analisar valores**. As questões desse tipo envolvem, com frequência, uma das duas situações a seguir:

1. encontrar um exemplo de polinomio que satisfaça uma propriedade es pecífica definida no enunciado;
2. provar que o polinomio não existe.

Analisemos, em detalhes, cada um dos casos citados.

2.1 Exemplo:

(IMO / SL - 2005) Sejam a,b,c,d,e,f números inteiros positivos. Sabendo $S = a+b+c+d+e+f$ divide tanto $(abc+def)$ como $(ab+bc+ca-de-ef-fd)$ prove que S é composto.

Solução Consideremos o polinômio:

$$P(x) = (x+a)\cdot(x+b)\cdot(x+c)\cdot(x-d)\cdot(x-e)\cdot(x-f)$$

$$= Sx^2 + Qx + R$$

sendo $Q = (ab+bc+ca-de-ef-fd)$ e $R = abc+def$. Daí, temos que:

$$S \mid Q, \quad R \Rightarrow S \mid P(x), \quad \forall x \in \mathbb{Z}$$

$$\Rightarrow S \mid P(d) = (d+a)\cdot(d+b)\cdot(d+c)$$

Por outro lado, como a,b,c,d são inteiros positivos, temos que:

$$S > \max\{d+a, d+b, d+c\} \Rightarrow S \nmid d+a, \quad S \nmid d+b, \quad S \nmid d+c$$

Portanto, S é composto, pois, caso contrário, pelo fato de $S \mid P(d)$, então ele dividiria pelo menos um elemento do conjunto $\{d+a, d+b, d+c\}$.

Notemos que, a partir de uma análise curta e descuidada do enunciado da questão anterior, ela não parece ser uma questão de polinômio. Daí, ressaltamos que essa velha questão clássica de que somente o treino exaustivo de questões pode levar um aluno a ser mais experiente nas questões de olimpíada de matemática.

Para não ficarmos induzidos a sempre pensar que toda questão de polinômio começa sempre com a tomada de um polinômio "esperto", estudemos a subseção a seguir.

Provar que o polinômio não existe

Vietnã/2017. Existe algum polinômio $P(x)$ com coeficientes inteiros que satisfaz:

$$\begin{cases} P(1+\sqrt{2}) = 1+\sqrt{2} \\ P(1+\sqrt{5}) = 2+3\sqrt{5} \end{cases}$$

Solução Suponha que existe tal polinômio. Considere a substituição $Q(x) = P(1+x) - 1$. Daí, temos que $Q(x)$ é um polinômio com coeficientes inteiros tal que:

$$\begin{cases} Q(\sqrt{2}) = \sqrt{2} \\ Q(\sqrt{5}) = 1+3\sqrt{5} \end{cases}$$

Do primeiro resultado, temos que $\sqrt{2}$ é raiz de $Q(x) - x$. Como o polinômio minimal de $\sqrt{2}$ é $x^3 - 2$, então temos que $x^3 - 2 \mid Q(x) - x$. Em outras palavras, podemos afirmar que existe um polinômio $R(x)$ com coeficientes inteiros tal que:

$$Q(x) - x = (x^3 - 2) \cdot R(x)$$

Como $R(x)$ tem coeficientes inteiros, então temos que existem a, b inteiros tais que $R(\sqrt{5}) = a + b\sqrt{5}$. Daí, substituindo $x = \sqrt{5}$ em todas as equações já destacadas até aqui, podemos concluir que:

$$Q(\sqrt{5}) - \sqrt{5} = \left[(\sqrt{5})^3 - 2\right] \cdot (a + b\sqrt{5})$$

$$1 + 3\sqrt{5} - \sqrt{5} = (5\sqrt{5} - 2) \cdot (a + b\sqrt{5})$$

$$1 + 2\sqrt{5} = (25b - 2a) + (5a - 2b)\sqrt{5}$$

Daí, temos que:

$$(25b - 2a) \cdot 1.5$$

$$(5a - 2b) \cdot 2 = 121b = 9 \Rightarrow b \notin \mathbb{Z}$$

Concluindo, portanto, um absurdo!

Notemos que, na solução anterior, foram importantes conceitos como manipulação algébrica (substituição de polinômios) e polinômio minimal. Aproveitemos, então, para ressaltar a importância do conhecimento teórico de polinômios para a melhor compreensão dos assuntos desse material.

3 Analisar alguma propriedade polinomial

Em algumas questões de polinomios com TN, não estamos interessados em analisar os valores em busca de provar a existência ou não de um polinomio, mas de analisar outras propriedades relacionadas a polinomios como, por exemplo, as raízes.

3.1 Exemplos:

(Belarus/2017) Seja $a_n \cdots a_1 a_0$ a representação decimal de 65^k para algum $k \geq 2$. Prove que o polinômio $a_n x^n + \cdots + a_1 x + a_0$ não possui raízes racionais.

Solução Suponha que há raiz. Como todos os a_i's são não negativos, então, se há raiz, ela é negativa. Daí, seja $\frac{p}{q}$ uma de tais raízes com p, q inteiros não negativos e $\gcd(p,q) = 1$. Daí, temos que:

$$P(x) = a_n\left(-\frac{p}{q}\right)^n + \cdots + a_1\left(-\frac{p}{q}\right) + a_0 = 0$$

Pelo algoritmo de divisão de polinômios, existem b_i's racionais $(0 \leq i < n-1)$ tais que:

$$P(x) = a_n x^n + \cdots + a_1 x + a_0 = (qx+p)\cdot(b_{n-1}x^{n-1} + \cdots + b_1 x + b_0) \tag{1}$$

sendo

$$\begin{cases} a_0 = p \cdot b_0 \\ a_n = q \cdot b_{n-1} \\ a_i = p \cdot b_i + q \cdot b_{i-1}, \quad \forall 1 \leq i \leq n-1 \end{cases} \tag{2}$$

Provemos que os b_i's são inteiros. Para isso, da recorrência anterior, podemos concluir que:

$$b_i = a_i \cdot \frac{1}{p} - a_{i-1} \cdot \frac{q}{p^2} + a_{i-2} \cdot \frac{q^2}{p^3} - \cdots + (-1)^i \cdot a_0 \cdot \frac{q^i}{p^{i+1}}, \quad \forall 0 \leq i \leq n-1$$

Portanto, podemos concluir que:

$$b_i \in \mathbb{Z} \Leftrightarrow p^{i+1} \mid a_i \cdot p^i - a_{i-1} \cdot p^{i-1} \cdot q + \cdots + (-1)^i \cdot a_0 \cdot q^i$$

Sendo tal fato verdadeiro a partir de $(5.2) \to q^n$.
Agora, calculemos alguns a_i's e b_i's pequenos. De $65^k = a_n \ldots a_1 a_0$, temos que:

$$\boxed{a_0 = 5} \qquad \boxed{a_1 = 2}$$

$$\boxed{a_2 = \begin{cases} 2, & \text{se } k = 2 \\ 6, & \text{se } k \geq 3 \end{cases}}$$

Fazendo $x = 10$ em (5.3), temos que:

$$P(10) = 65^k = (10q+p)\cdot[100 \cdot Q(10) + 10b_1 + b_0] \tag{3}$$

sendo $Q(x) = b_{n-1} \cdot x^{n-3} + \cdots + b_3 \cdot x^2 + b_2$ um polinômio com coeficientes inteiros.
São fatos conhecidos relacionados às raízes dos polinômios:

$$\begin{cases} p \mid a_0 \Rightarrow p \mid 5 \Rightarrow p = 1 \text{ ou } p = 5 \\ q \mid a_n \text{ e } a_n \text{ é dígito} \Rightarrow q \leq a_n \leq 9 \end{cases}$$

Daí, finalmente, temos dois casos para concluir a questão:
Caso 1: Se $p = 1$**:**
De (5.5), temos que $(10q+1) \mid 65^k$.

Por outro lado, $1 \leq q \leq 9$. Daí, olhando todos os $(10q+1)$'s, vemos que esse caso não gera solução.

Caso 2: Se $p = 5$ De (5.5), temos que $(10q+5) \mid 65^k$.

Por outro lado, $1 \leq q \leq 9$. Daí, olhando todos os $(10q+5)$'s, vemos que esse caso ainda poderia gerar duas soluções: $q = 2$ ou $q = 6$. Analisemos cada um desses casos:

Caso 2.1: Se $q = 2$ De (5.4), temos que:

$$\begin{aligned} a_0 &= p \cdot b_0 \quad (\text{com } (a_0, p) = (5,5)) \quad b_0 = 1 \\ a_1 &= p \cdot b_1 + q \cdot b_0 \quad (\text{com } (a_1, p, q) = (2,5,2)) \quad b_1 = 0 \\ a_2 &= p \cdot b_2 + q \cdot b_1 \quad (\text{com } (a_2, p, q, b_1) = (2,5,2,0)) \\ 2 &= 5 \cdot b_2 + 0 \Rightarrow b_2 \notin \mathbb{Z} \end{aligned}$$

Caso 2.2: Se $q = 6$ De (5.4), temos que:

$$\begin{aligned} a_0 &= p \cdot b_0 \quad (\text{com } (a_0, p) = (5,5)) \quad b_0 = 1 \\ a_1 &= p \cdot b_1 + q \cdot b_0 \quad (\text{com } (a_1, p, q) = (2,5,6)) \\ 2 &= 5 \cdot b_1 + 6 \Rightarrow b_1 \notin \mathbb{Z} \end{aligned}$$

Concluindo, assim, o absurdo.

Nem sempre as questões de polinômios com teoria dos números exigem tantos conhecimentos técnicos de polinômios. Às vezes, é necessário o contrário: muito conhecimento de teoria dos números e pouco de polinômios. Para entender melhor quando pode ocorrer esse segundo caso, iremos para a próxima subseção.

4 Analisar alguma propriedade de TN

Em outras questões, apesar de envolverem polinômios, o objetivo é estudar alguma propriedade relacionada a TN.

4.1 Exemplos

(Bulgária/2018) Dado um polinômio $P(x) = a_d x^d + \cdots + a_2 x^2 + a_0$ com coeficientes inteiros positivos e grau $d \geq 2$, considere a sequência:

$$\begin{aligned} b_1 &= a_0 \\ b_{n+1} &= P(b_n), \quad \forall n \geq 1 \end{aligned}$$

Prove que $\forall n \geq 2$ existe um número primo p tal que p divide b_n e não divide $b_1, \ldots, b_{n-1}$.

Solução Suponha que não existe tal primo. Daí, temos que existe $n > 2$ tal que para todo fator primo $p \mid b_n$ implica que $p \mid b_j$ para algum $1 \leq j \leq (n-1)$. Tome p um fator primo de b_n e seja $b_n = p^r \cdot \ell$, com $\gcd(p, \ell) = 1$. Daí, temos que:

$$\begin{aligned} b_{n+1} &= P(b_n) \\ &= a_d \cdot (p^r \cdot \ell)^d + \cdots + a_2 \cdot (p^r \cdot \ell)^2 + a_0 \\ &\equiv a_0 = b_1 \pmod{p^{r+1}} \end{aligned}$$

Analogamente, por indução, podemos concluir que:

$$b_{n+i+1} = P(b_{n+i}) \equiv P(b_i) = b_{i+1} \pmod{p^{r+1}}$$

e, portanto, por indução, segue que:

$$b_n \equiv b_{2n} \equiv \cdots \equiv b_{kn} \equiv \ldots \pmod{p^{r+1}}$$

Sendo $v_p(b_n) = r$, conclui-se que:

$$r = v_p(b_n) = v_p(b_{2n}) = \cdots = v_p(b_{kn}) = \ldots$$

Seja j tal que $p \mid b_j$ para algum $1 \leq j \leq (n-1)$. Analogamente, temos que:

$$v_p(b_j) = v_p(b_{2j}) = \cdots = v_p(b_{kj}) = \ldots$$

E consequentemente, podemos concluir que:

$$r = v_p(b_n) = v_p(b_{jn}) = v_p(b_j) \Rightarrow \boxed{v_p(b_j) = r}$$

Portanto, para todo fator primo p de b_n, temos que existe um j, com $1 \leq j \leq (n-1)$, tal que $v_p(b_n) = v_p(b_j)$. Daí, temos que:

$$b_n \mid b_1 \cdot b_2 \cdots b_{n-1} \Rightarrow \boxed{b_n \leq b_1 \cdot b_2 \cdots b_{n-1}}$$

Por outro lado, temos que:

$$b_n = P(b_{n-1}) > b_{n-1}^2 \Rightarrow b_{n-1} < \sqrt{b_n}$$

De forma análoga, por indução, podemos concluir que:

$$b_{n-k} < \sqrt{b_{n-k+1}} < \sqrt[4]{b_{n-k+2}} < \cdots < b_n^{\frac{1}{2^k}}$$

Daí, fazendo um produto telescópico, temos que:

$$0 < b_1 \cdot b_2 \cdots b_{n-1} < b_n^{\sum_{k=1}^{n-1} \frac{1}{2^k}} < b_n$$

Fato esse que é absurdo com (5.6).

Notemos que a questão anterior era basicamente uma questão de sequências com TN que envolvia quase nenhum conhecimento de polinômio. Por causa disso, algumas questões que aparentemente envolvem sequências e TN, sem parecerem envolverem polinômios, aparecerão na lista de exercícios extras. Há inclusive algumas que resolvem de forma semelhante a resolvida aqui. 1'1aq33we

5 Problemas

Problema 1. (Canadá/2013) Determine todos os polinômios $P(x)$ com coeficientes reais tais que:

$$(x+1)P(x-1) - (x-1)P(x)$$

seja um polinômio constante.

Problema 2. (Lusofonia/2016) Suponha que um número real α é raiz de um polinômio com coeficientes inteiros $P(x) = a_n x^n + \cdots + a_1 x + a_0$. Defina:

$$G = |a_n| + |a_{n-1}| + \cdots + |a_1| + |a_0|.$$

Dizemos que G é um gingado de α. Qual é o quarto maior número real α tal que 3 é um gingado de α?

Problema 3. (Rússia/2006) Considere um trinômio quadrático da forma $f(x) = x^2 + ax + b$. Sabe-se que a equação $f(f(x)) = 0$ possui quatro soluções reais diferentes e que a soma de duas delas é igual a -1. Prove que $b \leq \frac{1}{4}$.

Problema 4. (Hong Kong/TST - 2018) Encontre todos os polinômios P com coeficientes inteiros não negativos tais que $P(1) = 7P(2) = 2017$.

Problema 5. (Grécia/2017) Seja u a raiz positiva da equação $x^2 + x - 4 = 0$. Sendo n um inteiro positivo, sabe-se que o polinômio:

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

tem coeficientes inteiros não negativos e $P(u) = 2017$.

(a) Prove que $a_0 + a_1 + \cdots + a_n \equiv 1 \pmod 2$.

(b) Encontre o valor mínimo possível da expressão $a_0 + a_1 + \cdots + a_n$.

Problema 6. (Polônia/2016) Seja p um número primo. Encontre todos os números não negativos n para os quais o polinômio:

$$P(x) = x^4 - 2(n+p)x^2 + (n-p)^2$$

pode ser reescrito como produto de dois polinômios quadráticos P_1 e P_2, sendo ambos polinômios com coeficientes inteiros.

Problema 7. (Belarus/2019) Encontre todos os polinômios $P(x)$ e $Q(x)$ com coeficientes reais tais que:

$$P(Q(x)) = P(x) \cdot Q(x)^2.$$

Problema 8. (Vietnã/2019) Tome o polinômio $f(x) = x^2 - \alpha x + 1$, com $\alpha \in \mathbb{R}$.

(a) Para $\alpha = \frac{\sqrt{15}}{2}$, escreva $f(x)$ como quociente de dois polinômios com coeficientes não negativos.

(b) Determine todos os valores de α para os quais $f(x)$ pode ser escrito como quociente de dois polinômios com coeficientes não negativos.

6 Bibliografia

6.1 MARTINEZ, Fabio Brochero; et al. Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro. 3 ed. Rio de Janeiro: IMPA, 2013.

6.2 Teoria dos Números do Zero ao IME ITA Cone Sul EGMO - Armando Barbosa

6.3 Polos Olímpicos de Treinamento Intensivo (POTI)