Polinômios

E Z fez Q[x] a sua imagem e semelhança.

Diversas propriedades aritméticas dos inteiros traduzem-se quase literalmente para polinômios. Por exemplo, podemos definir divisibilidade de polinômios em $\mathbb{Q}[x]$ (i.e., com coeficientes racionais) da seguinte forma:

> *Sejam* $D(x), A(x) \in \mathbb{Q}[x]$. *Dizemos que* $D(x)$ *divide* $A(x)$, *e escrevemos* $D(x)|A(x)$, *se, e somente se, existe um polinômio* $B(x) \in \mathbb{Q}[x]$ *tal que* $A(x) = B(x) \cdot D(x)$.

Da mesma forma, definimos $A(x) \equiv B(x) \pmod{M(x)} \iff M(x)|A(x) - B(x)$. É claro que, com estas definições, as propriedades usuais se mantêm. Por exemplo, podemos mostrar que $x^n - 1|x^m - 1$ se $n|m$ da seguinte maneira:

$$\begin{aligned} x^n \equiv 1 \pmod{x^n - 1} &\implies (x^n)^{m/n} \equiv 1^{m/n} \pmod{x^n - 1} \\ &\iff x^m \equiv 1 \pmod{x^n - 1} \\ &\iff x^n - 1|x^m - 1 \end{aligned}$$

Algumas coisas precisam ser ligeiramente modificadas. A divisão euclidiana de $A(x)$ por $B(x)$, por exemplo, escreve-se agora

$$A(x) = B(x) \cdot Q(x) + R(x), \qquad \partial R(x) < \partial B(x) \text{ ou } R(x) = 0,$$

onde $\partial P(x)$ denota o *grau* de $P(x)$. Uma vez definida a divisão euclidiana, podemos aplicar o algoritmo de Euclides para obter o *mdc* de dois polinômios, definido como o polinômio mônico (i.e., de coeficiente líder 1) de maior grau que divide ambos os polinômios. Calculemos o $\mathrm{mdc}(x^3 - 3, x^2 + x + 2)$:

$$\begin{aligned} x^3 - 3 &= (x^2 + x + 2)(x - 1) - x - 1 \\ x^2 + x + 2 &= (-x - 1)(-x) + 2 \end{aligned}$$

Logo $\mathrm{mdc}(x^3 - 3, x^2 + x + 2) = \mathrm{mdc}(x^2 + x + 2, -x - 1) = \mathrm{mdc}(-x - 1, 2) = 1$. Assim, $x^3 - 3$ e $x^2 + x + 2$ são *primos entre si*.

Se quisermos determinar agora uma solução de $(x^3 - 3) \cdot A(x) + (x^2 + x + 2) \cdot B(x) = 1$, basta "reverter" o processo:

$$\begin{aligned} \begin{cases} -x - 1 = x^3 - 3 - (x^2 + x + 2)(x - 1) \\ 2 = x^2 + x + 2 - (-x - 1)(-x) \end{cases} &\implies 2 = x^2 + x + 2 - (x^3 - 3 - (x^2 + x + 2)(x - 1))(-x) \\ &\iff 2 = x(x^3 - 3) + (x^2 + x + 2)(-x^2 + x + 1) \\ &\iff 1 = \frac{x}{2} \cdot (x^3 - 3) + (x^2 + x + 2)\left(\frac{-x^2 + x + 1}{2}\right) \end{aligned}$$

O processo acima permite mostrar que se $A(x)$ e $B(x)$ são primos entre si, então existem $M(x)$ e $N(x)$ tais que $A(x) \cdot M(x) + B(x) \cdot N(x) = 1$. Daí, multiplicando a equação anterior por $C(x)$, podemos concluir que se $A(x)|B(x) \cdot C(x)$ e $\mathrm{mdc}(A(x), B(x)) = 1$, então $A(x)|C(x)$. Este fato é crucial na demonstração do *teorema da fatoração única*. Antes de formulá-lo, devemos definir o análogo de um primo para polinômios. Dizemos que um polinômio $P(x) \in \mathbb{Q}[x]$ é *irredutível em* $\mathbb{Q}$ se ele não pode ser escrito como produto de polinômios em $\mathbb{Q}[x]$ de graus menores do que $\partial P(x)$. Agora, podemos enunciar o importante

Teorema da Fatoração Única: *Todo polinômio não nulo em* $\mathbb{Q}[x]$ *fatora-se como produto de polinômios irredutíveis em* $\mathbb{Q}$. *Esta fatoração é única a menos da ordem dos fatores e da multiplicação por constante racional não nula.*

Temos também o simples porém muito útil

Teorema do Fator: *Se* $P(a) = 0$ *então* $x - a|P(x)$.

Basta escrever $P(x) = (x - a)Q(x) + r$ e substituir $x = a$.

Exemplo

Seja $f(x)$ um polinômio de coeficientes inteiros. Se $f(x) = 2$ para três inteiros distintos a, b e c, prove que $f(x)$ não pode ser igual a 3 para nenhum inteiro x.

Solução

Observe que $f(x)-2$ tem raízes distintas a, b e c, logo admite fatoração $f(x)-2=(x-a)(x-b)(x-c)g(x)$, onde $g(x)\in Z[x]$. Se $f(n)=3$ para algum inteiro n, teríamos $1=(n-a)(n-b)(n-c)g(n)$, o que é absurdo, pois 1 não pode ser escrito como produto de mais de dois inteiros distintos.

▸ **PROBLEMA 1**

(a) Determine $A(x)\in Q[x]$ tal que

$$A(x)(x^2+5)\equiv 1 \pmod{x^5+x+1}$$

(b) Determine $P(x)\in Q[x]$ tal que

$$\begin{cases} P(x)\equiv 1 \pmod{x^2+1} \\ P(x)\equiv 2x+3 \pmod{x^3+x^2+1} \end{cases}$$

(Isto não lembra algum teorema chinês de restos?)

Obviamente não há nada de especial no conjunto de coeficientes Q. Em seu lugar, podemos utilizar R, C e até mesmo Z/pZ, o conjunto dos inteiros módulo p, onde p é primo.

▸ **PROBLEMA 2**

Determine todos os naturais n tais que

$$x^n\equiv 1 \pmod{x^2+950x+1},$$

onde os polinômios estão em $Z/1999Z[x]$.

Em muitos casos, é conveniente substituir x pela raiz de um polinômio, anulando as partes indesejáveis.

Exemplo

Determine o resto da divisão do polinômio $(\cos\varphi+x\,\mathrm{sen}\,\varphi)^n$ por (x^2+1), onde n é um número natural.

Solução

O resto é da forma $ax+b$. Escrevendo $(\cos\varphi+x\,\mathrm{sen}\,\varphi)^n=(x^2+1)Q(x)+ax+b$ e substituindo $x=i$, obtemos $a=\mathrm{sen}\,n\varphi$ e $b=\cos n\varphi$.

Particularmente importante são as substituições por *raízes da unidade*. Veja o

Exemplo

Prove que para cada inteiro positivo n, existem polinômios $f,g\in Z[x]$ tais que

$$f(x)(x+1)^{2^n}+g(x)(x^{2^n}+1)=2$$

Solução

Vamos resolver o caso particular $n=1$ para ver o que está acontecendo.

$$f(x)(x+1)^2+g(x)(x^2+1)=2$$

A substituição óbvia aqui é $x=i$, o que nos leva a

$$f(i)(1+i)^2=2 \iff f(i)=\frac{2}{(1+i)^2}=-i$$

Então podemos tomar $f(x)=-x$. Mas e quanto a $g(x)$? Calma, as coisas foram feitas para funcionar! Observe que

$$2-f(x)(x+1)^2=2+x(x+1)^2 \tag{$*$}$$

admite raiz i e (automaticamente) raiz $-i$, logo é divisível por x^2+1 e o polinômio $g(x)$ nada mais é do que o quociente de $(*)$ por x^2+1.

No caso geral, consideremos no lugar de $\pm i$ as raízes de $x^{2^n}+1$. Observe que as raízes de $x^{2^n}+1 = (x^{2^{(n+1)}}-1)/(x^{2^n}-1)$ são as raízes $2^{(n+1)}$-ésimas da unidade que não são raízes 2^n-ésimas da unidade. Assim, sendo ζ uma raiz $2^{(n+1)}$-ésima primitiva da unidade, temos

$$x^{2^n}+1 = \prod_{\substack{1\leqslant k\leqslant 2^{(n+1)}\\ \text{k ímpar}}} (x-\zeta^k)$$

Substituindo $x=-1$, temos

$$(-1)^{2^n}+1 = \prod_{\substack{1\leqslant k\leqslant 2^{(n+1)}\\ \text{k ímpar}}} (-1-\zeta^k) \iff 2 = \prod_{\substack{1\leqslant k\leqslant 2^{(n+1)}\\ \text{k ímpar}}} (1+\zeta^k)$$

Basta mostrar que $1+\zeta$ "divide" cada $1+\zeta^k$. Mas isto é fácil:

$$\frac{1+\zeta^k}{1+\zeta} = \zeta^{k-1}-\zeta^{k-2}+\cdots+1$$

Portanto existe $f(x)$ tal que $2-f(x)(x+1)^{2^n}$ admite raízes ζ^k, k ímpar. Logo é divisível por $x^{2^n}+1$, concluindo a demonstração.

▶ **PROBLEMA 3**

Se $P(x)$, $Q(x)$, $R(x)$ e $S(x)$ são polinômios tais que

$$P(x^5)+xQ(x^5)+x^2R(x^5) = (x^4+x^3+x^2+x+1)S(x)$$

prove que $x-1$ é um fator de $P(x)$.

Irredutibilidade em Z é a mesma coisa que irredutibilidade em Q. É o que diz o

Lema de Gauß: *Seja* $f(x)$ *um polinômio em* $Z[x]$ *tal que* $f(x)$ *é irredutível em* $Z[x]$*, então* $f(x)$ *é irredutível em* $Q[x]$.

Provaremos, inicialmente, que se $C(x) = A(x)\cdot B(x)$, o mdc dos coeficientes de $A(x)$ é 1 e o mdc dos coeficientes de $B(x)$ também é 1, o mesmo vale para os coeficientes de $C(x)$. Seja

$$A(x) = a_0+a_1x+\cdots+a_nx^n$$
$$B(x) = b_0+b_1x+\cdots+b_nx^n$$

Considere um primo p e sejam i e j os menores tais que $p \nmid a_i$ e $p \nmid b_j$. Então p divide todos os termos de $c_{i+j} = a_0b_{i+j}+a_1b_{i+j-1}+\cdots+a_{i+j}b_0$, com exceção de a_ib_j. Logo $p \nmid c_{i+j}$, portanto o mdc dos coeficientes de $C(x)$ não é divisível por p para nenhum primo, logo é igual a 1 e o resultado segue.

Agora, suponha que $C(x) = \frac{P}{M}A(x)\cdot\frac{Q}{N}B(x)$, onde $A(x), B(x), C(x) \in Z[x]$, os coeficientes de $A(x)$ e os de $B(x)$ têm mdc 1 e $P, Q, M, N \in Z$. Como o mdc dos coeficientes de $A(x)\cdot B(x)$ é igual a 1, PQ/MN é o mdc dos coeficientes de $C(x)$ e é, portanto, um inteiro. Logo, se $C(x)$ é redutível em Q, é redutível em Z, completando a demonstração.

Uma técnica muito útil para provar que polinômios são irredutíveis em Z (e, portanto em Q) é "reduzi-lo" módulo um primo conveniente.

Exemplo

(IMO) Seja $n>1$ um inteiro e seja $f(x) = x^n+5x^{n-1}+3$. Prove que não existem polinômios g e h em Z, de graus maiores ou iguais a um, tais que $f(x) = g(x)\cdot h(x)$.

Solução

Se $f(x) = a(x)\cdot b(x)$, temos

$$f(x) \equiv a(x)\cdot b(x) \pmod{3} \iff x^{n-1}(x-1) \equiv a(x)\cdot b(x) \pmod{3}$$

É fácil verificar que f não tem raízes racionais (mas não acredite em mim; faça as contas você mesmo!). Logo pela fatoração única em $Z/3Z$, temos, sem perda de generalidade, que $a(x) \equiv x^j \pmod{3}$ e $b(x) \equiv x^{n-j-1}(x-1) \pmod{3}$, com $1<j<n-1$. Isto é um absurdo, já que os coeficientes independentes de $a(x)$ e $b(x)$ seriam divisíveis por 3, mas o coeficiente independente de $f(x)$ não é divisível por 9.

▸ **PROBLEMA 4**

Demonstre o *critério de irredutibilidade de Eisenstein:* se $p(x) = p_0 + p_1x + p_2x^2 + \cdots + p_nx^n$ é um polinômio de coeficientes inteiros tais que existe um primo p satisfazendo

(i) $p|p_i$ para $0 \leqslant i < n$ e $p \nmid p_n$ e

(ii) $p^2 \nmid p_0$,

então $p(x)$ é irredutível em $Z[x]$ (e, portanto, em $Q[x]$.)

▸ **PROBLEMA 5**

(a) Mostre que $(x+1)^{2^n} \equiv x^{2^n} + 1 \pmod{2}$.

(b) Mostre que o número de coeficientes binomiais ímpares entre $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$, é $2^{f(n)}$, onde $f(n)$ é o número de dígitos 1 na expansão binária de n.

▸ **PROBLEMA 6**

Mostre que para qualquer inteiro positivo n o polinômio $f(x) = (x^2 + x)^{2^n} + 1$ não pode ser decomposto como o produto de dois polinômios não constantes de coeficientes inteiros.

Muitas vezes, é conveniente considerar o *polinômio minimal* de α, isto é, o polinômio mônico em $Q[x]$ de menor grau que admite α como raiz. Temos o seguinte resultado interessante:

Polinômio Minimal: *Se $f(x) \in Q[x]$ é o polinômio minimal de α e $g(x) \in Q[x]$ é tal que $g(\alpha) = 0$, então $f(x)|g(x)$.*

A prova deste resultado é muito simples; basta dividir $g(x)$ por $f(x)$:

$$g(x) = f(x) \cdot q(x) + r(x), \qquad \partial r(x) < \partial f(x) \text{ ou } r(x) = 0$$

Substituindo $x = \alpha$, temos que $r(\alpha) = 0$. Como f é polinômio minimal, temos que $r(x) = 0$, completando a demonstração.

Exemplo

Sejam $M(x)$ e $N(x)$ polinômios irredutíveis mônicos de $Q[x]$. Suponha que M e N têm raízes α e β, respectivamente, tais que $r = \alpha + \beta$ é racional. Prove que $M^2(x) - N^2(x)$ tem uma raiz racional.

SOLUÇÃO

Temos que $N(r - x)$ é um polinômio em $Q[x]$ admitindo raiz α; logo $M(x)|N(r - x)$. Analogamente $N(x)|M(r - x)$. Comparando os graus, temos, portanto, que $M(x) = \pm N(r - x)$. Assim, $M^2(x) - N^2(x)$ admite a raiz racional $r/2$.

▸ **PROBLEMA 7**

Seja $f(x)$ um polinômio de coeficientes racionais e α um número real tal que

$$\alpha^3 - 1992\alpha = (f(\alpha))^3 - 1992 \cdot f(\alpha) = -33.$$

Prove que, para todo $n \geqslant 1$,

$$(f^{(n)}(\alpha))^3 - 1992 \cdot f^{(n)}(\alpha) = -33,$$

onde $f^{(n)}(\alpha) = \underbrace{f(f(\ldots f}_{n \text{ vezes}}(\alpha)))$, e n é um inteiro positivo.

▸ **PROBLEMA 8**

(OBM) Prove que nenhuma raiz do polinômio $G(x) = x^5 - x^4 - 4x^3 + 4x^2 + 2$ é raiz n-ésima de um número racional, $n > 1$ $(n \in N)$.

(Dica: com o auxílio do lema de Gauss, prove que $G(x)$ é irredutível em $Q[x]$. Então mostre que, se uma raiz n-ésima de um racional é raiz de $G(x)$, é também raiz de um polinômio de grau 4 em $Z[x]$, chegando a uma contradição.)

Particularmente útil é escrever um polinômio utilizando o

Polinômio Interpolador de Lagrange. *Seja* $p(x)$ *um polinômio de grau* n *e sejam* a_1, a_2, $\ldots$ a_{n+1} *reais distintos. Definimos*

$$L_i(x) = \prod_{\substack{1 \leqslant k \leqslant n+1 \\ k \neq i}} \frac{x - a_k}{a_i - a_k}.$$

Então

$$p(x) = \sum_{1 \leqslant i \leqslant n+1} L_i(x) \cdot p(a_i)$$

Exemplo

Seja $P(x)$ um polinômio satisfazendo

$$P(k) = \binom{n+1}{k}^{-1}, \qquad k = 0, 1, \ldots, n.$$

Determine $P(n+1)$.

Solução

Escrevemos $P(x) = \sum_{0 \leqslant k \leqslant n} \frac{L_k(x)}{\binom{n+1}{k}}$, onde $L_k(x)$ é definido como acima para $a_1 = 0$, $a_2 = 1$, $\ldots$, $a_{n+1} = n$. Observe que $L_k(n+1) = \binom{n+1}{k}(-1)^{n-k}$, logo $P(n+1) = 1$ se n é par e $P(n+1) = 0$ se n é ímpar.

▸ **PROBLEMA 9**

Sejam $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ um polinômio com coeficientes reais e x_1, x_2, $\ldots$, x_{n+1} inteiros distintos. Prove que $|f(x_k)| \geqslant n!/2^n$ para algum k, $1 \leqslant k \leqslant n$.