Polinômios irredutíveis

Sérgio Tadao Martins

23 de janeiro de 2009

1 Introdução: polinômios em uma variável

Um *polinômio* de grau n em uma variável x é uma expressão da forma

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \qquad a_n \neq 0.$$

Os coeficientes $a_0, a_1, \ldots, a_n$ são, geralmente, elementos de algum domínio de integridade (sem entrar em grandes detalhes, isso é só um jeito muito chique de dizer que podemos somar e multiplicar os coeficientes). Para nós, os coeficientes estarão quase sempre em um dos seguintes conjuntos: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (com p um número primo). É comum usarmos a notação $\mathbb{Z}[x]$ para o conjunto dos polinômios com coeficientes inteiros, $\mathbb{Q}[x]$ para o conjunto dos polinômios com coeficientes racionais, etc.

Vale destacar que o grau do polinômio $p(x)$ não está bem definido se $p(x) = 0$, o polinômio nulo. Apenas por uma questão de conveniência, vamos definir o grau do polinômio nulo como sendo $-\infty$ (isso pode parecer tudo, menos conveniente).

Sabemos como somar e multiplicar polinômios: a soma de dois polinômios é feita somando termos de mesmo grau, e a multiplicação é feita usando a propriedade distributiva:

$$\left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

$$\left(\sum_{i=0}^{m} a_i x^i\right) \cdot \left(\sum_{j=0}^{n} b_j x^j\right) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j\right) x^k.$$

Exemplo: Considere o polinômio $(x+1) \in \mathbb{Z}_2[x]$. Temos

$$(x+1)^2 = x^2 + 2x + 1 = x^2 + 1,$$

pois $2 \equiv 0 \pmod 2$.

O que veremos é que os polinômios são, de certa maneira, muito semelhantes aos números inteiros. Grande parte dessa semelhança segue do fato de existir, para polinômios, uma divisão euclidiana da mesma maneira que esta existe para os números inteiros.

2 Divisibilidade e divisão euclidiana

Passemos então a explorar as semelhanças entre os polinômios e os números inteiros. Vamos assumir que os polinômios mencionados pertencem todos a $R[x]$, em que R é um domínio de integridade. Para facilitar, podemos imaginar que R é um dos conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$.

Definição 1 *Dados polinômios $d(x)$ e $a(x)$ pertencentes a $R[x]$, dizemos que $d(x)$ divide $a(x)$ (e usamos a notação $d(x)|a(x)$) se existe um polinômio $c(x) \in R[x]$ tal que $a(x) = d(x)c(x)$.*

Esta relação de divisibilidade possui as mesmas propriedades que são válidas para os números inteiros. Em particular, se $d(x)|a(x)$ e $d(x)|b(x)$, então $d(x)|a(x)c_1(x)+b(x)c_2(x)$ para quaisquer $c_1(x)$ e $c_2(x)$.

Com a relação de divisibilidade entre polinômios, podemos definir o mdc de dois polinômios. Dados $a(x)$ e $b(x)$, dizemos que $d(x)$ é um mdc de $a(x)$ e $b(x)$ se:

1. $d(x)|a(x)$;
2. $d(x)|b(x)$;
3. $d(x)$ tem grau máximo entre todos os polinômios que cumprem as duas condições anteriores.

Exemplo: Vamos ver um exemplo em $\mathbb{Q}[x]$: sendo $a(x) = x^2 + 4x + 3$ e $b(x) = x^2 + 3x + 2$, é fácil ver que $d(x) = x + 1$ divide $a(x)$ e $b(x)$. Além disso, como $a(x) = (x + 1)(x + 3)$ e $b(x) = (x+1)(x+2)$, também não é difícil ver que a condição 3 da definição de mdc é satisfeita. Assim, $d(x)$ é um mdc dos polinômios $a(x)$ e $b(x)$, e podemos escrever $\text{mdc}(x^2+4x+3, x^2+3x+2) = x+1$.

Note que dissemos, na definição e no exemplo acima, *um* mdc, e não *o* mdc. No exemplo, note que o polinômio $d'(x) = 3x + 3$ também satisfaz as 3 condições que definem o mdc e, de maneira mais geral, o polinômio $r(x + 1)$ também, para qualquer r racional. Por isso dizemos *um* mdc, e não *o* mdc. Mesmo assim, se são dados dois polinômios e queremos nos referir ao mdc deles, é comum escolhermos como sendo o mdc o polinômio mônico, isto é, cujo coeficiente do termo de maior grau é igual a 1.

Talvez não seja tão óbvio como calcular o mdc de dois polinômios dados, mas na prática isto é bastante simples, pois podemos usar o algoritmo de Euclides (sim, aqui podemos inserir o comentário padrão "exatamente como nos números inteiros"). Apenas um detalhe merece ser comentado: para podermos efetuar a divisão entre polinômios, é necessário que os coeficientes do polinômio pertençam a um corpo. Isto quer dizer que devemos ser capazes de dividir um elemento por outro que não seja nulo. Por exemplo, teremos a divisão euclidiana em $\mathbb{Q}[x]$, pois se dividirmos um número racional por outro não nulo, obtemos um número racional. Mas, por outro lado, não podemos fazer o mesmo em $\mathbb{Z}[x]$: a divisão de dois números inteiros pode não ser um número inteiro.

Assim, estabelecemos agora a seguinte convenção: daqui em diante, a letra K representará para nós um corpo, e observamos que $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{Z}_p$ são corpos.

Teorema 2 (Divisão Euclidiana) *Sejam $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ e $b(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ polinômios de graus n e m em $K[x]$, respectivamente. Existem únicos polinômios $q(x)$ e $r(x)$ tais que $a(x) = b(x)q(x) + r(x)$, com o grau de $r(x)$ menor que o grau de $b(x)$.*

Demonstração: Considere o conjunto $S = \{a(x) - b(x)p(x) \ : \ p(x) \in K[x]\}$, e seja $r(x)$ um polinômio de grau mínimo que pertence a S. Temos então

$$a(x) = b(x)q(x) + r(x)$$

para algum $q(x) \in K[x]$. Vamos mostrar que o grau de $r(x)$ é menor que m. Suponha que

$$r(x) = c_t x^t + c_{t-1}x^{t-1} + \cdots + c_0,$$

com $c_j \in K$ e $c_t \neq 0$ se $t \neq 0$. Se $t \geq m$, então

$$a(x) - b(x)q(x) - \left(\frac{c_t}{b_m}\right) x^{t-m} b(x) = r(x) - \left(\frac{c_t}{b_m}\right) x^{t-m} b(x),$$

que é um polinômio de grau menor que t, o grau de r, e o lado esquerdo da igualdade acima mostra que esse é um polinômio que pertence a S (basta colocar $b(x)$ em evidência nos dois últimos termos), absurdo, pois $r(x)$ tem o menor grau entre todos os polinômios de S. Isso mostra que o grau de $r(x)$ é menor que m.

Agora a unicidade. Se

$$a(x) = b(x)q_1(x) + r_1(x) \quad \text{e} \quad a(x) = b(x)q_2(x) + r_2(x),$$

temos $b(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$. Mas o grau de $r_2(x) - r_1(x)$ é menor que o grau de $b(x)$, logo a última igualdade só pode ser verdadeira se $q_1(x) - q_2(x) = 0$, e consequentemente $r_2(x) - r_1(x) = 0$.

■

Até o momento temos tratado polinômios como objetos puramente formais, mas é claro que a cada polinômio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ associamos uma função polinomial

$$\begin{aligned} p\colon K &\to K \\ k &\mapsto (a_n k^n + a_{n-1}k^{n-1} + \cdots + a_1 k + a_0). \end{aligned}$$

Essa função polinomial simplesmente substitui o x por k e faz a conta. Dessa maneira temos o seguinte

Corolário 3 *Um elemento $a \in K$ é uma raiz de $p(x) \in K[x]$ se, e somente se, $(x-a)|p(x)$.*

Demonstração: Se $(x-a)|p(x)$, então existe $q(x) \in K[x]$ tal que $p(x) = q(x)(x-a)$, e portanto $p(a) = q(a)(a-a) = 0$, isto é, a é uma raiz de $p(x)$.

Suponha agora que $p(a) = 0$. Dividindo $p(x)$ por $(x-a)$, temos

$$p(x) = (x-a)q(x) + r(x),$$

em que $r(x)$ é um polinômio de grau menor que 1 (que é o grau de $x-a$). Mas então $r(x)$ é uma constante c. Re-escrevemos então

$$p(x) = (x-a)q(x) + c.$$

Substituindo x por a, ficamos com $0 = c$, pois a é raiz de $p(x)$, logo $(x-a)|p(x)$.

■

Exemplo: Considere o polinômio $(x^4 + 3x^3 + 2x + 4) \in \mathbb{Z}_5[x]$. Note que 1 é raiz deste polinômio: $1^4 + 3 \cdot 1^3 + 2 \cdot 1 + 4 \equiv 0 \pmod 5$. Portanto, ao dividirmos este polinômio por $x - 1$ em $\mathbb{Z}_5[x]$, devemos obter resto zero. Vamos fazer a divisão (usando o método de Briot-Ruffini):

1	1	3	0	2	4
	1	4	4	1	0

Assim, em $\mathbb{Z}_5[x]$ temos $x^4+3x^3+2x+4=(x-1)(x^3+4x^2+4x+1)$. Se prestarmos atenção, podemos ver que 1 é uma raiz de x^3+4x^2+4x+1 em $\mathbb{Z}_5[x]$, logo podemos continuar fatorando o nosso polinômio. Fica então um exercício: escrever x^4+3x^3+2x+4 como produto de polinômios de grau 1 em $\mathbb{Z}_5[x]$.

Se sabemos fazer a divisão euclidiana, calcular o mdc de dois polinômios dados fica uma moleza: realizamos divisões euclidianas sucessivas até obtermos resto zero. O último resto não nulo é um mdc dos polinômios dados.

Exemplo: Calculemos o $\mathrm{mdc}(x^3-3, x^2+x+2)$, em $\mathbb{Q}[x]$. Temos

$$x^3-3=(x^2+x+2)(x-1)-x-1$$
$$x^2+x+2=(-x-1)(-x)+2,$$

logo $\mathrm{mdc}(x^3-3, x^2+x+2)=\mathrm{mdc}(x^2+x+2,-x-1)=\mathrm{mdc}(-x-1,2)=1$

Mais ainda: se existe divisão euclidiana, automaticamente existe o teorema de Bézout:

Teorema 4 (Bézout) *Dados dois polinômios $a(x), b(x) \in K[x]$, existem polinômios $r(x), s(x)$ em $K[x]$ tais que $a(x)r(x)+b(x)s(x)=\mathrm{mdc}(a(x),b(x))$.*

Demonstração: "Exatamente como nos números inteiros". Aplicamos o algoritmo de Euclides e em seguida revertemos os passos.

■

Mais uma vez, cabe aqui o comentário padrão: tudo ocorre exatamente como nos números inteiros.

3 Polinômios irredutíveis

Depois desta breve introdução aos polinômios, finalmente vamos estudar os polinômios irredutíveis.

Definição 5 *Seja R um domínio de integridade. Dizemos que o polinômio não constante $p(x)$ é irredutível em $R[x]$ (ou irredutível sobre R) se é impossível expressar $p(x)$ como um produto $a(x)b(x)$ de dois polinômios $a(x)$ e $b(x)$ em $R[x]$ cujos graus são ambos maiores ou iguais a 1.*

Perceba que a definição diz "irredutível sobre R", e não simplesmente "irredutível". Não faz sentido dizer que um dado polinômio $p(x)$ é irredutível, simplesmente. Para nos convencermos disso, basta olharmos um exemplo. Seja $p(x)=x^2+1$. É fácil ver que $p(x)$ é irredutível sobre $\mathbb{R}$. De fato, se fosse possível escrever $x^2+1=(ax+b)(cx+d)$, com $(ax+b)$ e $(cx+d)$ de grau 1 e com coeficientes reais, então x^2+1 teria duas raízes reais, o que não é o caso. Por outro lado, sabemos que x^2+1 não é irredutível sobre $\mathbb{C}$, pois $x^2+1=(x+i)(x-i)$.

Exemplo: Vamos mostrar que $p(x)=x^3+3x+2$ é irredutível em $\mathbb{Z}_5[x]$. Se pudermos fatorar $x^3+3x+2=a(x)b(x)$ em $\mathbb{Z}_5[x]$, com $a(x)$ e $b(x)$ de grau maior ou igual a 1, então pelo menos um desses fatores deve ter grau 1. Podemos assumir, sem perda de generalidade, que o grau de $a(x)$ é 1, isto é, $a(x)=mx+n$, com $m \not\equiv 0 \pmod 5$. Isso implica que $-nm^{-1}$ é uma raiz de $a(x)$, e portanto também é uma raiz de $p(x)$. Porém, $p(0)=2$, $p(1)=1$, $p(2)=1$, $p(3)=3$, $p(4)=3$, isto é, $p(x)$ não possui raízes em $\mathbb{Z}_5$, logo é irredutível sobre $\mathbb{Z}_5$.

Polinômios irredutíveis são importantes porque eles representam, entre os polinômios, o mesmo papel que os números primos representam em $\mathbb{Z}$.

Teorema 6 *Seja $p(x)$ um polinômio irredutível em $K[x]$. Se $a(x), b(x) \in K[x]$ são tais que $p(x)|a(x)b(x)$, então $p(x)|a(x)$ ou $p(x)|b(x)$.*

Demonstração: Suponha que $p(x)$ não divide $a(x)$, e seja $d(x) = \text{mdc}(p(x), a(x))$. Como $p(x)$ é irredutível e não divide $a(x)$, o grau de $d(x)$ não pode ser maior do que zero. Logo $d(x) = 1$. Pelo teorema de Bézout, existem $r(x)$ e $s(x)$ tais que

$$a(x)r(x) + p(x)s(x) = 1.$$

Multiplicando a igualdade acima por $b(x)$ e observando que $p(x)|a(x)b(x) \Leftrightarrow a(x)b(x) = p(x)q(x)$ para algum $q(x)$, obtemos

$$a(x)b(x)r(x) + p(x)b(x)s(x) = b(x) \Longleftrightarrow p(x)(q(x)r(x) + b(x)s(x)) = b(x),$$

isto é, $p(x)|b(x)$.

■

Observe que o passo principal na demonstração acima é observar que $\text{mdc}(p(x), a(x)) = 1$. Assim, temos o seguinte resultado: se $p(x)|a(x)b(x)$ e $\text{mdc}(p(x), a(x)) = 1$, então $p(x)|b(x)$, com a mesma demonstração dada acima.

O próximo resultado é a versão para polinômios do Teorema Fundamental da Aritmética:

Teorema 7 *Todo polinômio de grau maior ou igual a 1 em $K[x]$ pode ser fatorado em $K[x]$ como um produto de polinômios irredutíveis. Esta fatoração é única, a menos da ordem dos fatores e da multiplicação por constantes não nulas de K.*

Demonstração: Seja $p(x) \in K[x]$ um polinômio de grau maior ou igual a 1. Se $p(x)$ for irredutível, não há o que fazer (ele já está fatorado como produto de irredutíveis). Caso contrário, escrevemos $p(x) = a(x)b(x)$, com $a(x)$ e $b(x)$ ambos de grau menor que o grau de $p(x)$. Se $a(x)$ e $b(x)$ forem irredutíveis, a fatoração termina. Caso contrário, repetimos este processo até obtermos uma fatoração de $p(x)$ como um produto de irredutíveis (o leitor mais experiente percebe que a formalização deste argumento involve uma indução finita, mas a ideia é clara).

Resta ainda mostrar a unicidade da fatoração. Suponha que

$$p(x) = q_1(x)q_2(x) \cdot \cdots \cdot q_m(x) = r_1(x)r_2(x) \cdot \cdots \cdot r_n(x) \tag{1}$$

são duas fatorações de $p(x)$ como produto de polinômios irredutíveis e $m \leq n$. É uma consequência do Teorema 6 que $q_1(x)$ divide algum dos polinômios $r_j(x)$, e podemos assumir sem perda de generalidade que $j = 1$. Então $q_1(x)|r_1(x)$. Mas $r_1(x)$ é irredutível, logo $r_1(x) = uq_1(x)$, com $u \in K$. Substituindo $r_1(x)$ em (1) e cancelando, ficamos com

$$q_2(x) \cdot \cdots \cdot q_m(x) = u_1 r_2(x) \cdot \cdots \cdot r_n(x).$$

Repetindo o argumento, eventualmente chegamos em

$$1 = u_1 \cdot \cdots \cdot u_m r_{m+1}(x) \cdot \cdots \cdot r_n(x),$$

o que só é possível se $m = n$. Logo os fatores irredutíveis $q_i(x)$ e $r_i(x)$ são os mesmos a menos da ordem e de constantes de K.

■

Quem fez o exercício proposto alguns parágrafos acima sabe que, em $\mathbb{Z}_5[x]$, $x^4+3x^3+2x+4 = (x-1)^3(x+1)$. Essa é uma decomposição em fatores irredutíveis. Uma outra fatoração em fatores irredutíveis só pode diferir dessa por constantes não nulas de $\mathbb{Z}_5[x]$. Por exemplo, temos também $x^4 + 3x^3 + 2x + 4 = (x-1)^2(2x-2)(3x+3)$.

4 Critérios de irredutibilidade

Em geral, decidir se um dado $p(x) \in K[x]$ é irredutível pode ser bastante difícil. Mas nem sempre! Por exemplo, é uma consequência do Teorema Fundamental da Álgebra que os únicos polinômios irredutíveis em $\mathbb{C}[x]$ são os polinômios de grau 1. Segue desse fato que os polinômios irredutíveis em $\mathbb{R}[x]$ têm grau 1 ou 2 (por quê?), e um polinômio $ax^2 + bx + c \in \mathbb{R}[x]$ de grau 2 é irredutível se, e somente se, $\Delta = b^2 - 4ac < 0$.

Quando consideramos polinômios em $\mathbb{Z}[x]$ ou $\mathbb{Q}[x]$, o problema fica bem mais difícil. Um dos resultados mais importantes é o seguinte:

Lema 8 (Gauss) *Se $p(x) \in \mathbb{Z}[x]$ é um polinômio irredutível sobre $\mathbb{Z}$, então $p(x)$ também é um polinômio irredutível sobre $\mathbb{Q}$.*

Este lema diz, simplesmente, que um polinômio de coeficientes inteiros que não pode ser fatorado como produto de polinômios com coeficientes inteiros também não pode ser fatorado como produto de polinômios com coeficientes racionais.

Demonstração: Em primeiro lugar, demonstraremos um resultado auxiliar. Um polinômio $f(x) \in \mathbb{Z}[x]$ é dito *primitivo* se o mdc dos seus coeficientes é igual a 1. Vamos agora provar o seguinte: se $f(x)$ e $g(x)$ são primitivos, então o produto $f(x)g(x)$ também é primitivo. De fato, suponha que $f(x)g(x)$ não é primitivo. Isto significa que existe um número primo p que divide todos os coeficientes de $f(x)g(x)$. Olhando os coeficientes de $f(x)g(x)$ módulo p, temos $f(x)g(x) = 0$ em $\mathbb{Z}_p[x]$. Isto implica, por p ser primo, que $f(x) = 0$ em $\mathbb{Z}_p[x]$ ou $g(x) = 0$ em $\mathbb{Z}_p[x]$. O primeiro caso quer dizer que todos os coeficientes de $f(x)$ são divisíveis por p, logo $f(x)$ não pode ser primitivo. E no segundo caso, $g(x)$ não pode ser primitivo. Assim, um produto de polinômios primitivos é necessariamente primitivo.

Agora provamos o resultado principal. Suponha que $p(x)$ pode ser fatorado sobre $\mathbb{Q}$, $p(x) = g(x)h(x)$. Sendo m_1 o mmc dos denominadores dos coeficientes em $g(x)$, temos $m_1 g(x)$ primitivo. Sendo m_2 o mmc dos denominadores dos coeficientes em $h(x)$, temos $m_2 h(x)$ primitivo. Temos então

$$m_1 m_2 p(x) = m_1 g(x) \cdot m_2 h(x).$$

O lado direito é primitivo, logo o lado esquerdo também deve ser. Isso só é possível se m_1 e m_2 são iguais a ± 1. Mas se m_1 e m_2 são ± 1, isso quer dizer que a nossa fatoração inicial já era uma fatoração em $\mathbb{Z}[x]$!

■

Exemplo: Mostremos que $p(x) = x^4 - 2x^2 + 8x + 1$ é irredutível sobre $\mathbb{Q}$. Pelo lema de Gauss, é suficiente ver que o polinômio é irredutível sobre $\mathbb{Z}$. Uma fatoração de $p(x)$ pode ser de dois tipos: um polinômio linear vezes um polinômio de grau 3, ou então o produto de dois polinômios quadráticos.

Se existe um polinômio linear que divide $p(x)$, isso quer dizer que $p(x)$ tem uma raiz racional. As únicas possíveis raízes racionais de $p(x)$ são 1 e -1, e podemos ver facilmente que nenhuma dela é raiz. Logo uma possível fatoração de $p(x)$ só pode ser um produto de dois polinômios quadráticos. Seja então

$$p(x) = (x^2 + ax + b)(x^2 + cx + d),$$

com a, b, c e d inteiros. Fazendo a distributiva e comparando coeficientes, temos

$$bd = 1 \quad ad + bc = 8 \quad ac + b + d = -2 \quad a + c = 0.$$

De $bd = 1$ temos $b = d = 1$ ou $b = d = -1$. Se $b = d = 1$, ficamos com $ac = -4$ e portanto $a = -c = \pm 2$ e não podemos ter $ad + bc = 8$. Se $b = d = -1$, obtemos $ac = 0$, logo $a = c = 0$ e novamente não temos $ad + bc = 8$. Portanto a fatoração como dois polinômios quadráticos também é impossível, e concluímos que o polinômio $p(x)$ é irredutível sobre $\mathbb{Q}$.

Outro critério de irredutibilidade muito útil é o seguinte:

Teorema 9 (Eisenstein) *Seja $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ um polinômio de grau n. Se existe um número primo p tal que $a_n \not\equiv 0 \pmod{p}$, $a_i \equiv 0 \pmod{p}$ para $0 \leq i \leq n-1$ e $a_0 \not\equiv 0 \pmod{p^2}$, então $p(x)$ é irredutível sobre $\mathbb{Z}$ (e portanto irredutível sobre $\mathbb{Q}$ também).*

Demonstração: Suponha que possamos fatorar $p(x)$ em $\mathbb{Z}[x]$:

$$p(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0),$$

com $b_r, c_s \neq 0$ e $r, s < n$. Como $a_0 \not\equiv 0 \pmod{p^2}$, b_0 e c_0 não podem ser ambos divisíveis por p. Suponha então que $p|c_0$, e seja m o menor valor de k tal que $c_k \not\equiv 0 \pmod{p}$. Temos então $m \geq 1$ e

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + b_{m-i} c_i,$$

para algum i, $0 \leq i < m$. Como b_0 e c_m não são divisíveis por p, e c_{m-1}, $\ldots$, c_i são todos divisíveis por p, temos $a_m \equiv b_0 c_m \not\equiv 0 \pmod{p}$. Logo $m = n$, o que implica $s = n$, um absurdo, pois supusemos $s < n$.

■

Exemplo: O polinômio $x^3 - 2$ é irredutível sobre $\mathbb{Q}$. Para ver isso, basta aplicarmos o critério de Eisenstein com $p = 2$.

Uma técnica bastante útil para provar que um polinômio é irredutível sobre $\mathbb{Z}$ (logo sobre $\mathbb{Q}$ também), é considerá-lo módulo p, para algum primo p conveniente, e usar fatoração única em $\mathbb{Z}_p[x]$.

Exemplo: Mostremos que $x^4 + x^3 + 5$ é irredutível sobre $\mathbb{Q}$. Uma maneira de fazer isso é a seguinte. Suponha que $x^4 + x^3 + 5 = f(x)g(x)$ com $f(x), g(x) \in \mathbb{Z}[x]$. Aqui, parece adequado considerar tudo módulo 5. Em $\mathbb{Z}_5[x]$, temos

$$x^4 + x^3 + 5 = x^3(x + 1).$$

Assim, devemos ter $f(x) = x^k + 5p(x)$ e $g(x) = x^{3-k}(x + 1) + 5q(x)$ para algum k, $1 \leq k \leq 2$ (por que o k não pode ser 0 ou 3?). Mas então o termo independente no produto $f(x)g(x)$ é divisível por 25, absurdo, pois $25 \not| 5$.

Esta mesma técnica pode ser usada para dar uma outra demonstração do critério de irredutibliidade de Eisenstein. Aliás, este é um dos problemas propostos!

Já que estamos sem medo de ir para $\mathbb{Z}_p[x]$ sempre que necessário, não poderíamos deixar de mencionar que, em $\mathbb{Z}_p[x]$, vale o "sonho de todo estudante":

Teorema 10 *Se p é primo e $a(x)$, $b(x)$ pertencem a $\mathbb{Z}_p[x]$, então*

$$(a(x) + b(x))^p = a(x)^p + b(x)^p.$$

Demonstração: Usando o binômio de Newton,

$$(a(x)+b(x))^p = \sum_{k=0}^{p} \binom{p}{k} a(x)^{p-k} b(x)^k.$$

Mas lembramos que

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \quad 0 \leq k \leq p,$$

logo $\binom{p}{k}$ é divisível por p para $1 \leq k \leq p-1$, pois o fator p do numerador não será cancelado. Sendo assim, em $\mathbb{Z}_p[x]$,

$$\sum_{k=0}^{p} \binom{p}{k} a(x)^{p-k} b(x)^k = a(x)^p + b(x)^p.$$

■

É claro que o teorema acima só vale em $\mathbb{Z}_p[x]$. Se ele valesse sempre, os alunos da 7^a série teriam vida bem mais fácil.

Finalmente, vamos ver um problema que usa todas essas ideias.

Exemplo: Mostremos que $f(x) = (x^2+x)^{2^n} + 1$ é irredutível sobre $\mathbb{Z}$ para todo n inteiro positivo.

Parece natural considerar o polinômio módulo 2. Em $\mathbb{Z}_2[x]$, temos $(x^2+x)^{2^n} + 1 = (x^2 + x + 1)^{2^n}$. Observe que polinômio x^2+x+1 é irredutível em $\mathbb{Z}_2[x]$ (isso é fácil de verificar).

Suponha que $(x^2+x)^{2^n}+1 = g(x)h(x)$, com $g(x), h(x) \in \mathbb{Z}[x]$. Pela fatoração de $(x^2+x)^{2^n}+1$ em $\mathbb{Z}_2[x]$, devemos ter, em $\mathbb{Z}[x]$, $g(x) = (x^2+x+1)^k + 2p(x)$ e $h(x) = (x^2+x+1)^{2^n-k} + 2q(x)$, para $1 \leq k < 2^n$.

Seja ω uma raiz de x^2+x+1. Temos $f(\omega) = (-1)^{2^n} + 1 = 2$ e, por outro lado, $f(\omega) = 4p(\omega)q(\omega)$. Dividindo $p(x)$ e $q(x)$ por x^2+x+1, obtemos

$$p(x) = (x^2+x+1)p_1(x) + (ax+b)$$
$$q(x) = (x^2+x+1)q_1(x) + (cx+d),$$

com a, b, c e d inteiros (como podemos garantir que são inteiros, e não simplesmente racionais?). Usando o fato que $\omega^2 = -\omega - 1$ segue que

$$2 = 4(a\omega+b)(c\omega+d) \iff \frac{1}{2} = ac\omega^2 + (ad+bc)\omega + bd \iff \frac{1}{2} = (ad+bc-ac)\omega + (bd-ac).$$

Como ω é irracional e $bd-ac$ é inteiro, a igualdade acima não pode ocorrer, absurdo. Logo $f(x)$ é irredutível sobre $\mathbb{Z}$. O único truque novo aqui consistiu em substituirmos uma raiz do polinômio x^2+x+1 para nos livrarmos de um trambolho indesejado.

5 Problemas

Evidentemente, nem tudo é uma moleza nesta vida. Existem muito mais coisas a serem ditas sobre polinômios, mas nada melhor do que praticar o que aprendemos. Para isso existem os problemas.

Problema 1 Se p é primo, mostre que $x^{p-1} + x^{p-2} + \cdots + x + 1$ é irredutível sobre $\mathbb{Q}$.

Problema 2 Dados polinômios $f_1(x)$, $f_2(x)$, ..., $f_n(x)$ em $\mathbb{Z}[x]$, mostre que existe um polinômio $g(x)$ redutível em $\mathbb{Z}[x]$ tal que $g(x) + f_i(x)$ é irredutível em $\mathbb{Z}[x]$ para todo i, $1 \leq i \leq n$.

Problema 3 Demonstre o critério de Eisenstein olhando o polinômio $p(x)$ como um elemento de $\mathbb{Z}_p[x]$ e usando fatoração única.

Problema 4 Representamos por $\mathbb{Z}[x, y]$ o conjunto dos polinômios nas variáveis x e y. Prove que

$$x^{200}y^5 + x^{51}y^{100} + x^{106} - 4x^{100}y^5 + x^{100} - 2y^{100} - 2x^6 + 4y^5 - 2$$

é irredutível em $\mathbb{Z}[x, y]$, isto é, não pode ser escrito como produto de dois polinômios de grau maior ou igual a 1 em $\mathbb{Z}[x, y]$. O grau de um polinômio de duas variáveis é calculdado da seguinte maneira: o termo $x^m y^n$ tem grau $m + n$, e o grau de um polinômio de duas variáveis é igual ao grau máximo que ocorre em seus termos. Por exemplo, o grau do polinômio dado é 205.

Problema 5 Seja $f(x) \in \mathbb{Z}[x]$ irredutível sobre $\mathbb{Z}$. Sabemos que $f(x)$ tem uma raiz α tal que $|\alpha| > \frac{3}{2}$. Prove que $f(\alpha^3 + 1) \neq 0$.

Problema 6 Seja $n > 1$ um inteiro e seja $f(x) = x^n + 5x^{n-1} + 3$. Prove que $f(x)$ é irredutível sobre $\mathbb{Z}$.

Problema 7 Prove que se a_1, a_2, ..., a_n são inteiros distintos, então $(x - a_1)^2(x - a_2)^2 \cdot \cdots \cdot (x - a_n)^2 + 1$ é irredutível sobre $\mathbb{Z}$.

Problema 8 Mostre que o polinômio $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ é irredutível sobre $\mathbb{Q}$ se a_0 é um número primo e $|a_0| > |a_1| + |a_2| + \cdots + |a_n|$.

Problema 9 Dado um número complexo α, o *polinômio minimal* de α é o polinômio mônico de $\mathbb{Q}[x]$ de menor grau que admite α como raiz (se tal polinômio existir!).

(a) Se $f(x) \in \mathbb{Q}[x]$ é o polinômio minimal de α, prove que $f(x)$ é irredutível em $\mathbb{Q}[x]$.

(b) Se $f(x) \in \mathbb{Q}[x]$ é o polinômio minimal de α e $g(x) \in \mathbb{Q}[x]$ é tal que $g(\alpha) = 0$, prove que $f(x)|g(x)$.

(c) Sejam $M(x)$ e $N(x)$ polinômios mônicos e irredutíveis em $\mathbb{Q}[x]$. Suponha que $M(x)$ e $N(x)$ tenham raízes α e β, respectivamente, tais que $\alpha + \beta \in \mathbb{Q}$. Prove que $M(x)^2 - N(x)^2$ possui uma raiz racional.