Polos Olímpicos de Treinamento
Curso de Álgebra - Nível 3
Prof. Cícero Thiago / Prof. Marcelo Mendes

Aula 12

Irredutibilidade de polinômios.

Continuaremos, neste artigo, trabalhando com polinômios em $\mathbb{Z}[x]$. Além disso,vamos dizer que um polinômio com coeficientes inteiros $P(x)$ é irredutível sobre $\mathbb{Z}$ se, e somente se, não for possível escrever $P(x)$ como produto de dois polinômios (não constantes) com coeficientes inteiros. Vamos começar com um problema de motivação!!

Problema 1. Prove que o polinômio

$$(x-a_1)(x-a_2)\dots(x-a_n)-1,$$

em que a_1, a_2, ..., a_n são inteiros distintos, não pode ser escrito como produto de dois polinômios não constantes com coeficientes inteiros, ou seja, é irredutível.

Solução.
Suponha, por contradição, que

$$f(x)=(x-a_1)(x-a_2)\dots(x-a_n)-1=p(x)q(x),$$

em que $p(x)$ e $q(x)$ são polinômios com coeficientes inteiros com grau menor que n. Então

$$g(x)=p(x)+q(x)$$

é um polinômio com coeficientes inteiros com grau menor que n. Então

$$p(a_i)q(a_i)=f(a_i)=-1$$

e ambos $p(a_i)$ e $q(a_i)$ são inteiros,

$$|p(a_i)|=|q(a_i)|=1$$

e

$$p(a_i)+q(a_i)=0.$$

Assim, $g(x)$ possui pelo menos n raízes. Mas o grau $g < n$, então $g(x) \equiv 0$. Então

$$p(x) = -q(x) \text{ e } f(x) = -p(x)^2,$$

implicando que o coeficiente líder de $f(x)$ é um número negativo, o que é impossível, pois o polinômio é mônico.

Teorema 1. (Critério de Einsenstein) Seja $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ um polinômio com coeficientes inteiros a_i e seja p um número primo que satisfaz as seguintes condições
(i) p não divide a_n;
(ii) p divide $a_0,\ a_1,\ \ldots, a_{n-1}$;
(iii) p^2 não divide a_0.
Então $P(x)$ é irredutível sobre $\mathbb{Z}$.

Demonstração. Suponha, por absurdo, que existem polinômios não constantes $F(x)$ e $G(x)$ com coeficientes inteiros tais que $P(x) = F(x)G(x)$. Logo,

$$P(x) = a_n x^n + \ldots + a_1 x + a_0$$

$$F(x) = b_s x^s + \ldots + b_1 x + b_0$$

$$G(x) = c_t x^t + \ldots + c_1 x + c_0.$$

Sem perda de generalidade podemos considerar que $s \leq t$, como $P(x) = F(x)G(x)$, ao realizarmos o produto poderemos comparar os coeficientes dos termos semelhantes, obtendo as seguintes igualdades

$$a_0 = b_0 c_0$$

$$a_1 = b_0 c_1 + b_1 c_0$$

$$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$$

$$\vdots$$

$$a_s = b_0 c_s + b_1 c_{s-1} + \ldots + b_{s-1} c_1 + b_s c_0$$

$$\vdots$$

$$a_t = b_0 c_t + b_1 c_{t-1} + \ldots + b_s c_{t-s}$$

$$\vdots$$

$$a_n = b_s c_t.$$

Por (ii) e (iii) temos que $a_0 = b_0 c_0$ é divisível por p e não é divisível por p^2, assim, exatamente um dos números b_0 e c_0 é divisível por p. Sem perda de generalidade suponha que p divide b_0 e que p não divide c_0.
Como p divide $a_1 = b_0 c_1 + b_1 c_0$ e b_0, então p divide $b_1 c_0$, porém como p não divide c_0, então

p divide b_1.
Portanto, raciocionando da mesma maneira, podemos demonstrar que p divide b_2, b_3, ..., b_{s-1} e b_s. Logo, p divide $b_s c_t = a_n$, contrariando (i).

Problema 2. Prove que o polinômio $P(x) = x^2 + x + 1$ é irredutível sobre $\mathbb{Z}$.

Solução. Não é difícil provar que $P(x)$ é irredutível sobre $\mathbb{Z}$ se, e somente se, $Q(x) = P(x+1)$ é irredutível sobre $\mathbb{Z}$, Logo

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

O primo $p = 3$ satisfaz o critério de Eisenstein, portanto $Q(x)$ é irredutível sobre $\mathbb{Z}$ e, com isso, $P(x)$ também será.

Problema 3. (TST Romênia) Sejam a, n números inteiros, e p um número primo tal que $p > |a| + 1$. Prove que o polinômio $f(x) = x^n + ax + p$ não pode ser representado como o produto de dois polinômios com coeficientes inteiros.

Solução. Seja z uma raiz complexa do polinômio. Vamos provar que $|z| > 1$. Suponha que $|z| \leq 1$, então $z^n + az = -p$, então:

$$p = |z^n + az| = |z||z^{n-1} + a| \leq |z^{n-1}| + |a| \leq 1 + |a|,$$

contrariando o fato que $p > |a|+1$. Agora, seja $f(x) = g(x)h(x)$ uma decomposição de $f(x)$ em polinômios com coeficientes inteiros então $p = g(0)h(0)$, então $|g(0)| = 1$ ou $|h(0)| = 1$. Suponha que $|g(0)| = 1$. Se $z_1,\ z_2,\ \ldots,\ z_k$ são raízes de $g(x)$ então são também raízes de $f(x)$, assim:

$$1 = |g(0)| = |z_1 z_2 \ldots z_k| = |z_1||z_2| \ldots |z_k| > 1,$$

que é uma contradição.

Exercícios Propostos

1. Prove que o polinômio
$$P(x) = x^{101} + 101x^{100} + 102$$
é irredutível em $\mathbb{Z}[x]$.

2. Prove que para todo número primo p, o polinômio
$$P(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$
é irredutível em $\mathbb{Z}[x]$.

3. Prove que para todo inteiro positivo n, o polinômio $P(x) = x^{2^n} + 1$ é irredutível em $\mathbb{Z}[x]$.

4. Prove que para quaisquer inteiros distintos a_1, a_2, ..., a_n o polinômio

$$P(x) = (x - a_1)^2(x - a_2)^2 \dots (x - a_n)^2 + 1$$

não pode ser escrito com um produto de dois polinômios não constantes com coeficientes inteiros.

5. Seja p um primo da forma $4k + 3$, k inteiro. Prove que para qualquer inteiro positivo n, o polinômio $(x^2 + 1)^n + p$ é irredutível em $\mathbb{Z}[x]$.

6. Seja p um número primo. Prove que o polinômio

$$P(x) = x^{p-1} + 2x^{p-2} + 3x^{p-3} + \ldots + (p-1)x + p$$

é irredutível sobre $\mathbb{Z}[x]$.

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

Bibliografia

1. III Olimpiada Nacional Escolar de Matematica - 2006
Jorge Tipe, John Cuya, Claudio Espinoza e Sergio Vera

2. Putnam and Beyond
Razvan Gelca e Titu Andreescu