

Aula de exercícios

Prof. Dr. Vinícius Wasques

Departamento de Matemática

Universidade Estadual Paulista “Júlio de Mesquita Filho” - UNESP.

<https://viniciuswasques.github.io/home/>

email: viniciuswasques@gmail.com

Teorema de Bachet-Bézout para polinômios

Se $f(x) = g(x) = 0$, então o resultado segue de modo trivial. Suponha então que os polinômios $f(x)$ e $g(x)$ sejam não nulos.

Seja o conjunto

$$I(f, g) = \{f(x)m(x) + g(x)n(x) \mid m(x), n(x) \in K[x]\}.$$

Seja $d(x) = f(x)m_0(x) + g(x)n_0(x)$ o polinômio mônico de menor grau no conjunto $I(f, g)$.

Veja que $d(x)$ divide todos os polinômios de $I(f, g)$. De fato, dado $p(x) = f(x)m(x) + g(x)n(x)$, sejam $q(x)$ e $r(x)$ tais que

$$p(x) = d(x)q(x) + r(x)$$

com $\deg r < \deg d$ (fato esse garantido pelo algoritmo da divisão).

Assim, $r(x) = p(x) - d(x)q(x) = f(x)m(x) + g(x)n(x) - (f(x)m_0(x) + g(x)n_0(x))q(x)$, logo

$$r(x) = f(x)(m(x) - m_0(x)q(x)) + g(x)(n(x) - n_0(x)q(x)) \in I(f, g)$$

Por outro lado, seja a o coeficiente líder de $r(x)$. Assim, se $r(x) \in I(f, g)$, também temos que $\bar{r}(x) = \frac{1}{a}r(x) \in I(f, g)$.

Portanto, temos que $\deg \bar{r} = \deg r < \deg d$ e mais, \bar{r} é mônico. Absurdo, pois o polinômio d é o único com tal propriedade.

Portanto, $r(x) = 0$ e temos que $d(x)$ divide todos os polinômios de $I(f, g)$.

Em particular, como $f(x)$ e $g(x)$ são elementos de $I(a, b)$ temos que $d(x)$ divide cada um deles. Logo, $\deg d(x) \leq \deg \text{mdc}(f(x), g(x))$.

Por outro lado, $\text{mdc}(f(x), g(x))$ divide $f(x)$ e $g(x)$, conseqüentemente, divide $f(x)m_0(x) + g(x)n_0(x) = d(x)$. Logo, $\deg \text{mdc}(f(x), g(x)) \leq \deg d(x)$.

Portanto, segue que $\deg \text{mdc}(f(x), g(x)) = \deg d(x)$ e assim,

$$f(x)m(x) + g(x)n(x) = d(x),$$

em que $d(x)$ é o máximo divisor comum entre $f(x)$ e $g(x)$.

Exercício 1.5, lista 6.

Podemos escrever $f(x) = x^{p-1} + \dots + x + 1$ como

$$f(x) = \frac{x^p - 1}{x - 1}$$

Assim,

$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-2} + \dots + \binom{p}{p-1} + \binom{p}{p} - 1$$

em que

$$\binom{n}{m} \stackrel{\text{def}}{=} \frac{n!}{m!(n-m)!}$$

Isto é,

$$f(x+1) = x^{p-1} + \binom{p}{1} x^{p-2} + \dots + \binom{p}{p-1}$$

Com exceção do coeficiente líder, todos os coeficientes deste polinômio são múltiplos de p , sendo que o termo independente $\binom{p}{p-1} = p$ não é múltiplo de p^2 .

Portanto, Pelo critério de Eisenstein, $f(x+1)$ é irredutível em $\mathbb{Z}[x]$ e, portanto, $f(x)$ também o é.

Sendo assim, pelo Lema de Gauss segue que o polinômio $f(x)$ é irredutível em $\mathbb{Q}[x]$