Teorema de Bachet-Bézout e Teorema Fundamental da Aritmética

Prof. Dr. Vinícius Wasques

Universidade Estadual Paulista "Júlio de Mesquita Filho" - Campus Rio Claro

15 de junho de 2020

Teorema de Bachet-Bézout

Sejam $a, b \in \mathbb{Z}$. Então existem $x, y \in \mathbb{Z}$ com

$$ax + by = mdc(a, b).$$

Portanto, se $c \in \mathbb{Z}$ é tal que $c|a$ e $c|b$, então $c|mdc(a, b)$

Demonstração

Se $a = b = 0$, então o problema está resolvido pois mdc(a,b)=0 e portanto para quaisquer $x, y \in \mathbb{Z}$ segue o resultado.

Demonstração

Se $a = b = 0$, então o problema está resolvido pois mdc(a,b)=0 e portanto para quaisquer $x, y \in \mathbb{Z}$ segue o resultado.

Caso contrário, considere o conjunto de todas as combinações $\mathbb{Z}$-lineares de a e b, isto é,

$$I(a, b) = \{ax + by : x, y \in \mathbb{Z}\}.$$

Demonstração

Se $a = b = 0$, então o problema está resolvido pois mdc(a,b)=0 e portanto para quaisquer $x, y \in \mathbb{Z}$ segue o resultado.

Caso contrário, considere o conjunto de todas as combinações $\mathbb{Z}$-lineares de a e b, isto é,

$$I(a, b) = \{ax + by : x, y \in \mathbb{Z}\}.$$

Exercício: Mostre que existe pelo menos um elemento positivo em $I(a, b)$

Seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a, b)$.

Note que d divide todos os elementos de $I(a, b)$. De fato, dado $m = ax + by \in I(a, b)$, e dividindo-o por d temos

$$m = dq + r \quad \text{e} \quad 0 \leq r < d,$$

com $q, r \in \mathbb{Z}$

Seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a, b)$.

Note que d divide todos os elementos de $I(a, b)$. De fato, dado $m = ax + by \in I(a, b)$, e dividindo-o por d temos

$$m = dq + r \quad \text{e} \quad 0 \leq r < d,$$

com $q, r \in \mathbb{Z}$

Assim,

$$r = m - dq = ax + by - (ax_0 + by_0)q = a(x - qx_0) + b(y - qy_0) \in I(a, b).$$

No entanto, como $r < d$ e d é o menor elemento positivo de $I(a, b)$, segue que $r = 0$ e portanto $d|m$.

Em particular, como $a, b \in I(a, b)$ temos que $d|a$ e $d|b$, logo $d \leq mdc(a, b)$.

Note ainda que se $c|a$ e $c|b$, então $c|ax_0 + by_0 \Leftrightarrow c|d$.

Tomando $c = mdc(a, b)$ temos que $mdc(a, b)|d$ o que, juntamente com a desigualdade $d \leq mdc(a, b)$, mostra que $d = mdc(a, b)$.

Corolário. Sejam $a, b, c \in \mathbb{Z}$. A equação

$$ax + by = c$$

admite solução inteira em x e y se, e somente se, $mdc(a, b)|c$

Corolário. Sejam $a, b, c \in \mathbb{Z}$. A equação

$$ax + by = c$$

admite solução inteira em x e y se, e somente se, $mdc(a, b)|c$

Dem: Se a equação admite solução inteira, então mdc(a, b) divide o lado esquerdo, logo deve dividir o direito também.

Corolário. Sejam $a, b, c \in \mathbb{Z}$. A equação

$$ax + by = c$$

admite solução inteira em x e y se, e somente se, $mdc(a, b)|c$

Dem: Se a equação admite solução inteira, então mdc(a, b) divide o lado esquerdo, logo deve dividir o direito também.

Reciprocamente, se $mdc(a, b)|c$, digamos $c = k.mdc(a, b)$ com $k \in \mathbb{Z}$, pelo teorema de Bachet-Bézout existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = mdc(a, b)$ e multiplicando tudo por k obtemos que $x = kx_0$ e $y = ky_0$ são soluções da equação dada.

Teorema Fundamental da Aritmética

Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma como um produto

$$n = p_1 \dots p_m$$

em que $m \in \mathbb{N}$ e $p1 \leq \dots \leq p_m$ são números primos.

Demonstração

Mostraremos a existência da fatoração de n em primos por indução forte.

Se n é primo não há o que provar (escrevemos m $= 1$, $p_1 =$ n).

Base da Indução: Como $n = 2$ e $n = 3$ são primos, começamos a base de indução por $n = 4 = 2.2$.

Hipótese de Indução: Suponha que a propriedade é verdadeira para todo natural k tal que $k \leq n$.

Seja n um número composto, isto é, existem $a, b \in \mathbb{N}$, com $1 < a < n$, $1 < b < n$ tal que $n = ab$.

Como a e b são menores que n, podemos aplicar a hipótese de indução sobre eles, isto é, a e b se decompõem como produto de primos

$$a = p_1.p_2 \ldots p_m \quad \text{e} \quad b = q_1.q_2 \ldots q_k.$$

Portanto, $n = ab = p_1.p_2 \ldots p_m.q_1.q_2 \ldots q_k$ pode ser escrito como produto de primos.

Pelo princípio de indução, esse fato é garantido para qualquer $n \in \mathbb{N}$.

Vamos agora mostrar a unicidade. Suponha por absurdo que n possui duas fatorações diferentes

$$n = p_1 \dots p_m = q_1 \dots q_l,$$

com $p_1 \leq \dots \leq p_m$, $q_1 \leq \dots \leq q_l$ e que n é mínimo com tal propriedade.

Como $p_1 | q_1 \dots q_l$ temos $p_1 | q_i$ para algum valor de i.

Vamos agora mostrar a unicidade. Suponha por absurdo que n possui duas fatorações diferentes

$$n = p_1 \dots p_m = q_1 \dots q_l,$$

com $p_1 \leq \dots \leq p_m$, $q_1 \leq \dots \leq q_l$ e que n é mínimo com tal propriedade.

Como $p_1 | q_1 \dots q_l$ temos $p_1 | q_i$ para algum valor de i.

Mostre que se p é primo e $p | q_1 \dots q_n$, então $p | q_i$ para algum algum $i \in \{1, \dots, n\}$.

Logo, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$.

Analogamente temos $q_1 \leq p_1$, assim $p_1 = q_1$. Note que

$$n/p_1 = p_2 \dots p_m = q_2 \dots q_l$$

admite uma única fatoração, pela minimalidade de n. Portanto,

$m = l$ e $p_i = q_i$ para todo i, o que contradiz o fato de n ter duas fatorações.

Existem infinitos números primos.

Existem infinitos números primos.

Demonstre o Teorema de Euclides.

Exercícios

Discutir os exercícios propostos nesse slide.

Discutir exercícios da Lista 1, disponível no site.

Focar a discussão na seção de divisibilidade.

Referências

MARTINEZ, F.E.B; MOREIRA, C.G.T; SALDANHA, N.,T.; TENGAN, E. Teoria dos Números. Um passeio com Primos e outros Números Familiares pelo Mundo Inteiro. IMPA, 2013.

GRAHAM, R. L., KNUTH, D. E., PATASHNIK, O Matemática Concreta. LTC, São Paulo, 1995

NIVEN, I. E.; ZUCKERMAN, N.S. An Introduction to the Theory of Numbers, NY, John Wiley & Sons, 1991.

Contato

Prof. Dr. Vinícius Wasques

email: viniciuswasques@gmail.com

Departamento de Matemática

site: `https://viniciuswasques.github.io/home/`