O Teorema de Bezout

Leonardo Carmo

Introdução

O teorema de Bachet-Bezout é um dos pilares da teoria dos números. Ele assegura a existência de soluções para equações específicas e possui diversas aplicações úteis em olimpíadas de matemática que serão apresentadas neste artigo. Encorajamos o leitor a pensar nos problemas resolvidos antes de ler as soluções.

O Teorema

Teorema 1. *(Teorema de Báchet-Bézout) Dados a, $b \in \mathbb{Z}$, $\exists\ x$, $y \in \mathbb{Z}$ tais que*

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

Demonstração. Consideremos o conjunto $K = \{at + bs \mid t,s \in \mathbb{Z}\}$. Como $|a| = a \cdot I + b \cdot 0 \in K$ em que $I = 1$ ou $I = -1$ dependendo do sinal de a, temos que $K \cap \mathbb{Z}^+ \neq \emptyset$, e portanto possui um menor elemento positivo. Chamemos esse elemento de d. Nós vamos mostrar que $d = mdc(a,b)$. Como $d \in K$, suponhamos $d = at_0 + bs_0$. Sendo r o resto na divisão de a por d, pelo algoritmo da divisão podemos escrever:

$$r = a - qd = a - q(at_0 + bs_0) = a(1 - qt_0) + b(-qs_0) \qquad 0 \leq r < d$$

Portanto $r \in K$, mas $r < d$, absurdo! O único caso é $r = 0 \implies a = qd$. Logo, $d \mid a$, e, com um raciocínio análogo, $d \mid b$. Agora, se M é um outro divisor comum de a e b, temos que $M \mid at_0 + bs_0 = d$, o que implica $|M| \leq |d|$ e portanto d é por definição o maior divisor comum entre a e b, o que conclui nossa demonstração. $\square$

Conseguimos achar soluções para equações que envolvem o $mdc(a,b)$, mas será que é possível achar para todo número? Existe uma cota a partir da qual todo inteiro positivo pode ser representado na forma $ax+by$? Os dois próximos poderosos teoremas respondem a essas perguntas:

Teorema 2. *Se c é um inteiro qualquer, existem inteiros x,y para o qual a equação*

$$ax + by = c$$

vale se e somente se $mdc(a,b) \mid c$.

Demonstração. Comecemos pela volta do teorema, ou seja, suponha que $d = mdc(a,b) \mid c$. Pelo teorema de Báchet-Bézout, existem u,v inteiros tais que

$$au + bv = d$$

Como $c = dk$, multiplicando ambos os lados por k nós obtemos:

$$a(uk) + b(vk) = dk = c$$

E portanto existem tais inteiros. Por outro lado, como $a = ds$ e $b = dr$, caso $ax + by = c$ nós teremos:

$$ax + by = c \iff d(sx + ry) = c \iff d = mdc(a,b) \mid c$$

o que conclui a prova. □

Definição 1. ***(Números Representáveis)*** *Dizemos que um inteiro positivo c é representável em (a,b) com a e b inteiros positivos e $mdc(a,b) = 1$ se existem inteiros não negativos (x,y) tais que $ax + by = c$*

Em particular, mostraremos que a partir de uma constante C, todo $X \geq C$ é representável em (a,b). Vamos determinar esta constante:

Lema 1. *Todo número inteiro $k \geq (a-1)(b-1)$ é representável em (a,b).*

Demonstração. Pelo **Teorema 2** nós asseguramos a existência de um par ordenado (x,y) de inteiros que satifazem a equação para um determinado número k. Como k é positivo, temos que x e y não podem ser ambos negativos. Caso ambos sejam positivos, o resultado segue. Caso contrário, observe que:

$$k = ax + by = (x - bt)a + (y + at)b$$

Ou seja, o par $(x - bt, y + at)$ também é solução para um determinado inteiro t . O lema se reduz a mostrar que existe um inteiro t tal que $x - bt > -1$ e $y + at > -1$, que é equivalente a:

$$\frac{x+1}{b} > t > \frac{-1-y}{a}$$

Isso decorre do fato do intervalo $\left(\frac{-1-y}{a}, \frac{x+1}{b}\right)$ ter tamanho maior que 1, pois:

$$\frac{x+1}{b} - \left(\frac{-1-y}{a}\right) = \frac{ax + by + a + b}{ab} \geq \frac{(a-1)(b-1) + (a+b)}{ab} = \frac{ab+1}{ab} > 1$$

□

Provamos com esse lema que todo número inteiro positivo maior que $ab-a-b$ é representável em (a,b). Mostraremos que o próprio número $ab-a-b$ não pode ser representado dessa forma.

Teorema 3. *(Teorema do Chicken McNugget) Dados dois inteiros positivos a,b com $mdc(a,b) = 1$, o maior número inteiro positivo não representável por (a,b) é $ab-a-b$*

Demonstração. Pelo **Lema 1** nós já mostramos que todo número maior que $ab-a-b$ funciona. Suponhamos por absurdo que $ab-a-b = ax+by$ com $x,y \geq 0$. Olhando módulo a, temos que $y \equiv -1$ e olhando módulo b temos $x \equiv -1$ também. Neste caso, $x \geq b-1$ e $y \geq a-1$, logo $ab-a-b = ax+by \geq a(b-1)+b(a-1) = 2ab-a-b > ab-a-b$, contradição. □

A seguir mostramos uma aplicação em uma OBM recente.

Problemas

Problema 1. *(OBM N3 2019/P4) Prove que para todo inteiro positivo m existe um inteiro positivo n_m tal que para todo inteiro positivo $n \geq n_m$, existem inteiros positivos (não necessariamente distintos) a_1, a_2, ..., a_n tais que*

$$\frac{1}{a_1^m} + \frac{1}{a_2^m} + \ldots + \frac{1}{a_n^m} = 1.$$

Demonstração. Comecemos percebendo que $a_1 = a_2 = \ldots = a_{p^m} = p$ é uma solução para essa equação. A ideia é particionar frações $\frac{1}{X^m}$ em uma soma de outras. Por exemplo:

$$\frac{1}{a_i^m} = \sum_{i=1}^{p^m} \frac{1}{(p \cdot a_i)^m}$$

$$\frac{1}{a_j^m} = \sum_{j=1}^{q^m} \frac{1}{(q \cdot a_j)^m}$$

Observe que a cada operação deste tipo para cada parcela a_i e a_j, o número de parcelas na soma aumenta de $p^m - 1$ e de $q^m - 1$, respectivamente. Isso significa que se fizermos x vezes a primeira operação e y vezes a segunda, o número de parcelas na soma aumentará de $x(p^m-1)+y(q^m-1)$.

Para que possamos utilizar o **Teorema 3**, tomemos $q = p^m - 1$, de forma que $mdc(p^m-1,q^m-1) = 1$.

Assim, se em determinado momento tínhamos P parcelas na soma, após as $x+y$ operações teremos $P' = P + x(p^m - 1) + y(q^m - 1)$ parcelas. Pelo teorema do Chicken McNugget, como $mdc(p^m - 1, q^m - 1) = 1$, segue que P' atinge todos valores a partir de uma determinada cota (em particular, vimos que tal cota seria $P + [(p^m - 1) - 1][(q^m - 1) - 1]$) e portanto o resultado segue. $\square$

Problema 2. *Quantos são os inteiros positivos que não são representáveis por* (a,b)*?*

Problema 3. *(OBM 2009): Mostre que existe um inteiro positivo* n_0 *com a seguinte propriedade: para qualquer inteiro* $n \geq n_0$*, é possível particionar um cubo em* n *cubos menores.*

Problema 4. *(IMO 1983): Sejam* a,b,c *inteiros positivos, dois a dois primos entre si. Prove que* $2abc - ab - bc - ca$ *é o maior inteiro que não pode ser escrito na forma* $xab + ybc + zca$*, onde* x,y,z *são inteiros não negativos.*

Problema 5. *(IMO 1996) Seja* $\mathbb{N}_0$ *o conjunto dos inteiros não negativos. Encontre todas as funções* $f : \mathbb{N}_0 \to \mathbb{N}_0$ *tal que*

$$f(m + f(n)) = f(f(m)) + f(n) \qquad \text{para todos } m, n \in \mathbb{N}_0.$$

Dicas e soluções

Problema 2. Prove que exatamente um dos números $k, ab - a - b - k$ é representável por a e b. O que isso implica sobre a quantidade de números não representáveis?

Problema 3. O problema é basicamente o mesmo que o da OBM de 2019 só que em uma versão simplificada. Tente assimilar essas ideias!

Problema 4. Para mostrar que $2abc - ab - bc - ca$ não funciona, olhe $moda$, $modb$ e $modc$ para achar um limitante inferior para x,y,z. Para mostrar que os outros números maiores podem ser representados, utilize a mesma ideia do Teorema do Chicken McNugget.

Problema 5. Cuidado! $f(n) = n$ não é a única solução. Prove que o menor elemento da imagem de f divide todos os outros deste mesmo conjunto, uma ideia muito parecido com a que utilizamos na demonstração do Teorema de Bezout.

Referências

[1] Elementary Number Theory - David M. Burton (1976)
[2] Bézout e Outros Bizus - Davi Lopes (18ª Semana Olímpica)