Diofantinas Lineares

Yvens Ian

26ª Semana Olímpica - 24 de janeiro de 2023

1 Introdução

Neste material estudaremos equações diofantinas lineares, que são equações do tipo

$$ax + by = n,$$

onde todas as variáveis são inteiras. Elas aparecem várias vezes em problemas diversos da matemática, e veremos aqui propriedades interessantes sobre elas, além de, claro, analisar suas soluções nos inteiros.

Primeiro, vamos ver um contexto, para facilitar. Imagine que João participa de um campeonato de Hipotetibol. Nesse jogo, se um participante ganha uma partida em menos de 1 minuto, ele recebe 5 pontos, se ganha em 1 minuto ou mais, recebe 3 pontos, porém, se perde em menos de 1 minuto, recebe -5 pontos, e se perde em 1 minuto ou mais, recebe -3 pontos. Dessa forma, qual seria uma boa maneira de contabilizar os pontos de João?

Podemos equacionar os pontos de João da seguinte forma, se x é a quantidade de partidas valendo 5 pontos que João ganhou a mais do que perdeu, e y quantas de 3 pontos João ganhou a mais que perdeu, então, a quantidade de pontos de João campeonato é

$$5x + 3y.$$

Note que x, y podem ser negativos, se João perde mais que ganha.

Agora, com essa pontuação, vêm perguntas clássicas à nossa mente (tente respondê-las!), por exemplo:

- Quais são todos os números que podem ser pontuações de João?
- Se soubermos a pontuação final de João, é possível determinar x, y?

A seguir, encontraremos formas de responder todas essas perguntas, mas de maneira geral, ou seja, com a equação $ax + by$ ao invés de $5x + 3y$. Onde a, b são inteiros positivos.

2 O Teorema de Bézout

Quais são todos os números que podem ser pontuações de João? Para responder essa pergunta de maneira geral, utilizaremos o Teorema de Bézout:

Teorema 1 (Teorema de Bézout) Dados a, b inteiros positivos, existem x, y inteiros tais que

$$ax + by = \text{mdc}\,(a, b).$$

E, além disso, mdc(a, b) é o menor inteiro positivo que pode ser escrito como combinação linear de a, b.

Prova: Seja X o conjunto de todos os números que podem ser escritos da forma $ax + by$ para algum par (x, y) de inteiros. Por exemplo, $a = a \cdot 1 + b \cdot 0$, $b = a \cdot 0 + b \cdot 1$, $a - b = a \cdot 1 + b \cdot (-1)$ estão todos no conjunto X. Seja, então, $d = ax_0 + by_0$ o menor número positivo que pertence a X.

A seguir, provaremos que d divide a e b.

Suponha, por absurdo, que d não divide a. Assim, pelo algoritmo da divisão, existem q, r inteiros positivos tais que $a = d \cdot q + r$ e $0 < r < d$. Porém,

$$d = ax_0 + by_0 \implies a = (ax_0 + by_0)q + r \implies r = b \cdot (-y_0 \cdot q) + a \cdot (1 - x_0 \cdot q),$$

ou seja, $r \in X$, então, como r é positivo, tem-se que $r \geq d$, pela minimalidade de d, porém, $d > r$, pela definição de r. Absurdo! Logo, $d|a$, e, analogamente, $d|b$.

Por fim, como $d|a$ e $d|b$, temos que $\text{mdc}\,(a, b) \geq d$, pela definição de mdc (**máximo** divisor comum). Porém,

$$d = ax_0 + by_0 \implies \frac{d}{\text{mdc}\,(a, b)} = \frac{a}{\text{mdc}\,(a, b)}x_0 + \frac{b}{\text{mdc}\,(a, b)}y_0 \in \mathbb{Z} \implies \text{mdc}\,(a, b)|d,$$

assim, $\text{mdc}\,(a, b) \geq d \geq \text{mdc}\,(a, b)$, e, portanto, $d = \text{mdc}\,(a, b)$.

Ou seja, existem x, y inteiros tais que $ax + by = \text{mdc}\,(a, b)$, e além disso, $\text{mdc}\,(a, b)$ é o menor inteiro positivo que pode ser escrito dessa forma. ■

Com isso, quais as possíveis pontuações de João? Note que

$$ax + by = \text{mdc}\,(a, b) \implies a \cdot (xk) + b \cdot (yk) = k \cdot \text{mdc}\,(a, b)$$

então, todos os múltiplos de $\text{mdc}\,(a, b)$ podem ser pontuações de João. Além disso, se $ax + by = n$ for uma pontuação de João,

$$n = ax + by \implies \frac{n}{\text{mdc}\,(a, b)} = \frac{a}{\text{mdc}\,(a, b)}x + \frac{b}{\text{mdc}\,(a, b)}y \in \mathbb{Z} \implies \text{mdc}\,(a, b)|n,$$

assim, n pode ser uma pontuação de João, ou seja, uma combinação linear de $a, b \iff n$ é múltiplo de $\text{mdc}\,(a, b)$.

3 Soluções de uma Diofantina Linear

Se soubermos a pontuação final de João, é possível determinar x, y? Não exatamente, pois existem infinitas soluções, mas podemos achar a família de pares (x, y) que satisfazem a equação com o seguinte lema:

Lema 1 (Solução de Diofantinas Lineares) A equação

$$ax + by = n$$

tem soluções inteiras (x, y) se, e somente se, $d = \text{mdc}(a, b)$ divide n. Sendo (x_0, y_0) uma dessas soluções, então os pares

$$(x_k, y_k) = \left(x_0 + k \cdot \frac{b}{d}, y_0 - k \cdot \frac{a}{d}\right),\ k \in \mathbb{Z}$$

representam todas as possíveis soluções dessa equação.

Prova: Já provamos anteriormente que o conjunto solução de $ax + by$ são todos os múltiplos de $\text{mdc}(a, b)$. Portanto, para todo n múltiplo de $\text{mdc}\,(a, b)$, temos que existe uma solução inicial (x_0, y_0). Assim,

$$ax + by = n = ax_0 + by_0 \iff$$
$$a(x - x_0) = b(y_0 - y) \iff$$
$$\frac{x - x_0}{y - y_0} = \frac{b}{a},$$

podemos, então, reduzir a fração do lado direito, deixando-a irredutível, dividindo o numerador b e o denominador a por $d = \text{mdc}\,(a, b)$,

$$\frac{x - x_0}{y - y_0} = \frac{\frac{b}{d}}{\frac{a}{d}} \iff$$
$$x - x_0 = k \cdot \frac{b}{d} \text{ e } y_0 - y = k \cdot \frac{a}{d}.$$

Assim, todas as soluções de $ax + by = n$ são

$$(x_k, y_k) = \left(x_0 + k \cdot \frac{b}{d}, y_0 - k \cdot \frac{a}{d}\right),\ k \in \mathbb{Z} \ \blacksquare$$

Voltando à pergunta inicial, sabendo somente a pontuação final de João, n, não conseguimos encontrar x, y. Porém, como conseguimos encontrar todas as possíveis soluções, basta alguma outra informação para encontrar o par original.

4 Problemas

Problema 1 Determine todas as soluções inteiras da equação $5x + 3y = 7$

Problema 2 Ache todas as soluções inteiras de $2x + 3y + 5z = 11$

Problema 3 Antônio e Bruno compraram ingressos para um evento. Ao chegarem em casa, eles perceberam que os ingressos eram numerados com valores naturais consecutivos. O número de Antônio é múltiplo de 27 e o número de Bruno é múltiplo de 25. Além disso, eles viram que os números dos ingressos são os menores naturais que satisfazem essas propriedades e que o número de Antônio é menor do que o de Bruno. Encontre os números dos ingressos e justifique sua resposta.

Problema 4 São dadas 10 caixas com algumas bolas dentro de cada (não necessariamente o mesmo número de bolas), seja n um inteiro positivo menor que 10 dado, uma operação consiste em escolher n caixas distintas e colocar mais uma bola dentro de cada uma dessas caixas.

1) Prove que se $n = 7$, então podemos aplicar um número finito de operações de forma que no fim todas as caixas tenham a mesma quantidade de bolas.

2) Prove que se $n = 8$, a afirmação de 1 nem sempre vale.

Problema 5 Prove que

$$\frac{\text{mdc}(m, n)}{n}\binom{n}{m}$$

pertence aos inteiros para todos os pares de inteiros $n \geq m \geq 1$.

Problema 6 Chame um conjunto A de inteiros de Legal se possui a seguinte propriedade:

Se $x, y \in A$ (possivelmente $x = y$), então, $x^2 + kxy + y^2 \in A$ para todo inteiro k.

Determine todos os pares m, n de inteiros diferentes de 0 tais que o único conjunto Legal contendo ambos m e n é o conjunto de todos os inteiros.

Problema 7 Prove que existe um inteiro positivo n_0 com a seguinte propriedade: para todo inteiro $n \geq n_0$ é possível particionar um cubo em n cubos menores.