Algoritmo de Euclides Estendido, Relação de Bézout e Equações Diofantinas

Relação de Bézout e Aplicações

Tópicos Adicionais

Algoritmo de Euclides Estendido, Relação de Bézout e Equações Diofantinas
Relação de Bézout e Aplicações

1 Exercícios Introdutórios

Exercício 1. Encontre inteiros a e b tais que

$$290a + 57b = 1$$

Exercício 2. Em cada item abaixo, encontre um inteiro positivo a tal que:

i) $2 \cdot a$ deixa resto 1 na divisão por 17.

ii) $3 \cdot a$ deixa resto 1 na divisão por 25.

iii) $5 \cdot a$ deixa resto 2 na divisão por 71.

Exercício 3. Em cada item abaixo, determine se existem inteiros a e b que satisfazem a equação dada.

a) $37a + 48b = 3$.

b) $99a + 57b = 5$.

c) $10a + 6b = 12$.

Exercício 4. Para cada um dos pares de inteiros abaixo (a, b), encontre x e y tais que $ax + by = 1$

(a) $(a, b) = (21n + 4, 14n + 3)$.

(b) $(a, b) = (2n + 13, n + 7)$.

(c) $(a, b) = (12n + 1, 30n + 2)$.

(d) $(a, b) = (4n + 3, 5n + 4)$

2 Exercícios de Fixação

Exercício 5. Sejam a, b, c, d inteiros não nulos tais que $ad - bc = 1$. Encontre inteiros x e y tais que

$$x(a + b) + y(c + d) = 1.$$

Exercício 6. Em Brasilândia, o jogo de basquete é jogado com regras diferentes. Existem apenas dois tipos de pontuações para as cestas: 5 e 11 pontos. É possível um time fazer 39 pontos em uma partida?

3 Exercícios de Aprofundamento e de Exames

Exercício 7. Mostre que existe um inteiro múltiplo de 241^2 e terminado em 241.

Exercício 8. Se $mdc(a, b) = 1$, mostre que no conjunto $\{a, 2 \cdot a, 3 \cdot a, \ldots, b \cdot a\}$ existe um número que deixa resto 1 por b.

Exercício 9. Mostre que se $mdc(a, b) = mdc(a, d) = mdc(c, b) = mdc(c, d) = 1$, então

a) $mdc(ac, bd) = 1$.

b) $mdc(a^n, b^m) = 1 \ \forall m, n \in \mathbb{N}$.

Exercício 10. Mostre que todo inteiro positivo k pode ser escrito (de modo único) de uma e, somente uma, das seguintes formas:

$$11y - 5x, \text{ ou } 11y + 5x, \text{ com } 0 \leq y < 5 \text{ e } x \geq 0$$

Exercício 11. Dados os inteiros positivos a e b com $mdc(a, b) = 1$, mostre que existem exatamente

$$\frac{(a-1)}{2} \cdot \frac{(b-1)}{2}$$

números inteiros não negativos que não são da forma $ay + bx$ com $x, y \geq 0$.

Exercício 12. Suponha agora que as pontuações das cestas do basquete de Brasilândia tenham mudado para a e b pontos com $0 < a < b$. Sabendo que existem exatamente 35 valores impossíveis de pontuações e que um desses valores é 58, encontre a e b.

Respostas e Soluções.

1. Como $mdc(290, 57) = 1$, aplicando o Algortimo de Euclides, obtemos as seguintes equações:

$$\begin{aligned} 290 &= (57 \cdot 5) + 5 \\ 57 &= (5 \cdot 11) + 2 \\ 5 &= (2 \cdot 2) + 1 \\ 2 &= (1 \cdot 2) + 0 \end{aligned}$$

As equações anteriores mostram que cada resto é uma combinação linear dos dividendos e divisores correspondentes. Por um processo de trocas sucessivas, podemos escrever o último resto não nulo como uma combinação linear do dividendo e do divisor da primeira equação:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - (57 - 5 \cdot 11) \cdot 2 \\ &= 5 \cdot 23 - 57 \cdot 2 \\ &= (290 - 57 \cdot 5) \cdot 23 - 57 \cdot 2 \\ &= 290 \cdot 23 - 57 \cdot 117. \end{aligned}$$

Portanto, $a = 23$ e $b = -117$.

2.

i) Aplicando o Algoritmo de Euclides, como $mdc(2, 17) = 1$, podemos encontrar a combinação linear:

$$2 \cdot 26 - 3 \cdot 17 = 1$$

, segue que $2 \cdot 26$ deixa resto 1 por 17 e $a = 26$ é uma solução.

ii) Aplicando o Algoritmo de Euclides, como $mdc(3, 25) = 1$, podemos encontrar a combinação linear:

$$3 \cdot 17 - 25 \cdot 2 = 1$$

, segue que $3 \cdot 17$ deixa resto 1 por 25 e $a = 17$ é uma solução.

iii) Aplicando o Algoritmo de Euclides, como $mdc(5, 71) = 1$, podemos encontrar a combinação linear:

$$5 \cdot 128 - 71 \cdot 9 = 1$$

, segue que $5 \cdot 256$ deixa resto 2 por 71 e $a = 256$ é uma solução.

3.

(a) Como $mdc(37, 48) = 1 \mid 3$, pelo Teorema de Bézout, existem inteiros a e b satisfazendo a equação.

(b) Como $mdc(99, 57) = 3 \nmid 5$, não existem inteiros a e b satisfazendo a equação.

(c) Como $mdc(10, 6) = 2 \mid 12$, existem inteiros a e b satisfazendo a equação.

4.

(a)

$$\begin{aligned} -2(21n + 4) + 3(14n + 3) &= -42n - 8 + 42n + 9 \\ &= 1. \end{aligned}$$

(b)

$$\begin{aligned} -1(2n + 13) + 2(n + 7) &= -2n - 13 + 2n + 14 \\ &= 1. \end{aligned}$$

(c)

$$\begin{aligned} 5(12n + 1) - 2(30n + 2) &= 60n + 5 - 60n - 4 \\ &= 1. \end{aligned}$$

(d)

$$\begin{aligned} -5(4n + 3) + 4(5n + 4) &= -20n - 15 + 20n + 16 \\ &= 1. \end{aligned}$$

5. Como $d(a + b) - b(c + d) = da - bc = 1$, basta escolher $x = d$ e $y = -b$.

6. Sejam x e y os números de cestas de 5 e 11 pontos, respectivamente. O problema se resume em decidir se existem inteiros não negativos x e y tais que $5x + 11y = 39$. Em vez de testarmos os valores de x e y, somemos $11 + 5$ em ambos os lados da equação:

$$5(x + 1) + 11(y + 1) = 55.$$

Como $5 \mid 55$ e $5 \mid 5(x + 1)$, segue que $5 \mid 11(y + 1)$ e, com mais razão, $5 \mid y + 1$ pois $mdc(5, 11) = 1$. Do mesmo modo, $11 \mid x + 1$. Assim,

$$55 = 5(x + 1) + 11(y + 1) \geq 5 \cdot 11 + 11 \cdot 5 = 110,$$

pois $x + 1, y + 1 \geq 1$. Essa contradição mostra que não é possível fazermos 39 pontos em uma partida.

7. Observe que um número termina em 241 se ele é da forma $1000x + 241$, com $x \in \mathbb{N}$. Pelo Teorema de Bézout, existem inteiros positivos a e b tais que $241b - 1000a = 1$. Daí, $241^2 b = 1000 \cdot 241a + 241$. Portanto, se $x = 241a$, o número $1000x + 241$ termina em 241 e é múltiplo de 241^2.

8. Suponha que dois elementos do conjunto mencionado possuem o mesmo resto na divisão por b, digamos $i \cdot a$ e $j \cdot a$, daí $b \mid i \cdot a - j \cdot a = a \cdot (i - j)$. Como $mdc(a, b) = 1$, segue que $b \mid i - j$. Entretanto, se $i \neq j$, $|i - j| \in \{1, 2, \ldots, b - 1\}$ e consequentemente $b \nmid i - j$. Esse absurdo mostra que os restos de todos os inteiros do conjunto dado na divisão por b são distintos. Como existem exatamente b restos possíveis, pelo menos um desses inteiros deverá deixar resto 1.

9.

(a) Pelo Teorema de Bézout, existem inteiros x, y, m, n tais que

$$\begin{aligned} ax + by &= 1 \\ am + dn &= 1. \end{aligned}$$

Portanto, $bd(ny) = (1 - ax)(1 - am) = 1 - a(m + x - amx)$ e $bd(ny) + a(m + x - amx) = 1$. Isso mostra que $mdc(a, bd) = 1$. Analogamente, $mdc(c, bd) = 1$. Se $bd = a'$, $a = b'$ e $c = d'$, como $mdc(d', a') = mdc(b', a') = 1$, o argumento inicial nos diz que $mdc(b'd', a') = 1$, ou seja, $mdc(ac, bd) = 1$.

(b) Pelo item anterior, se $c = 1$ e $b = d$, então $mdc(a, b^2) = 1$. Aplicando novamente o item anterior dessa vez trocando b por b^2 e fazendo $b = d$, podemos obter $mdc(a, b^3) = 1$. De modo análogo, aplicações sucessivas do item anterior produzem $mdc(a, b^m) = 1$ para todo $m \in \mathbb{N}$. Invertendo-se os papéis de a e b e novamente aplicando o item anterior, obtemos $mdc(a^n, b^m) = 1$.

10. Pelo Teorema de Bézout, existem m e n tais que $5m + 11n = 1$. Sejam q e r o quociente e resto da divisão de kn por 5, i.e., $kn = 5q + r,\ 0 \leq r < 5$. Assim,

$$\begin{aligned} k &= 5(km) + 11(kn) \\ &= 5(km) + 11(5q + r) \\ &= 5(km + 11q) + 11r. \end{aligned}$$

Basta fazer $x = km + 11q$ e $r = y$.

Para ver a unicidade, suponha que $11m \pm 5n = 11a \pm 5b$ com $0 \leq m, a < 5$. Então $11(m - a) = 5(\pm b \pm n)$. Usando que $mdc(11, 5) = 1$, segue que $5 \mid m - a$. A única opção é termos $m = a$, pois o conjunto $\{0, 1, 2, 3, 4\}$ contém cada um dos restos possíveis na divisão por 5. Consequentemente, $\pm 5n = \pm 5b$ e $n = b$.

Sendo assim, os elementos do conjunto

$$B(5, 11) = \{11y - 5x \in \mathbb{Z}_+^*; 0 \leq y < 5 \text{ e } x > 0\}$$

constituem o conjunto dos inteiros não negativos que não podem ser escritos como combinações lineares de 11 e 5 em inteiros não negativos. Seus elementos são:

$$\begin{aligned} y = 1 &\Rightarrow 11y - 5x = 1, 6 \\ y = 2 &\Rightarrow 11y - 5x = 2, 7, 12, 17 \\ y = 3 &\Rightarrow 11y - 5x = 3, 8, 13, 18, 23, 28 \\ y = 4 &\Rightarrow 11y - 5x = 4, 9, 14, 19, 24, 29, 34, 39 \end{aligned}$$

11. Repetindo o argumento do exercício anterior, como $mdc(a, b) = 1$, todo inteiro positivo k pode ser escrito (de modo único) de uma e, somente uma, das seguintes formas:

$$ay - bx, \text{ ou } ay + bx, \text{ com } 0 \leq y < b \text{ e } x \leq 0$$

Além disso, os elementos do conjunto

$$B(a, b) = \{ay - bx \in \mathbb{Z}_+^*; 0 \leq y < b \text{ e } x > 0\}$$

consite do conjunto de inteiros positivos que não são da forma $ay + bx$ com $x, y \geq 0$. Precisaremos agora de dois resultados:

i) Se $c \geq ab - a - b + 1$, como o conjunto $\{0a, a, 2a, 3a, \ldots, (b-1)a\}$ contém todos os restos na divisão por b, existe um deles, digamos ia, tal que $c - ia$ é múltiplo de b. Ou seja, $c - ia = mb$. Como $c \geq ab - a - b + 1$ e $i \leq b - 1$, segue que

$$\begin{aligned} mb &= c - ia \\ &> ab - a - b + 1 - (b-1)a \\ &= -b + 1 \end{aligned}$$

Como mb é um múltiplo de b maior que $-b + 1$, segue que $mb \geq 0$, ou seja, $c = ia + mb$ com $i, m \geq 0$ e $i < b$. Daí, $B(a, b) \subset \{1, 2, 3, \ldots, ab - a - b\}$

ii) Se $l \in \{0, 1, 2, \ldots, ab - a - b\}$, então l é da forma $ay + bx$ com $x, y \geq 0$ se, e somente se, $ab - a - b - l$ não é desta forma.

Suponha que l não é da forma $ay + bx$, com $x, y \geq 0$. Assim, pela observação inicial, l pode ser escrito de modo único como $ay - bx$ e $x > 0$ e $0 \leq y \leq b$. Daí

$$\begin{aligned} ab - a - b - l &= ab - a - b - (ay - bx) \\ &= a(b - y - 1) + b(x - 1). \end{aligned}$$

Como $y < b$ e $x > 0$, segue que $b - y - 1 \geq 0$ e $x - 1 \geq 0$. Reciprocamente, se $l = ay + bx$, com $x, y \geq 0$, então pela observação inicial podemos supor ainda que $y < b$. Daí

$$\begin{aligned} ab - a - b - l &= ab - a - b - (ay + bx) \\ &= a(b - y - 1) - b(x + 1). \end{aligned}$$

Como $0 \leq b - y - 1 \leq b - 1$ e, em virtude da unicade mencionada no início, podemos garantir que $ab - a - b - l$ não é uma combinação linear não negativa de a e b.

O último resultado nos permite criar pares da forma $(l, ab - a - b - l)$ contendo exatamente um inteiro que não é uma combinação linear não negativa de a e b. Assim, dado que o conjunto $0, 1, 2, \ldots, ab - a - b$ contém $(a-1)(b-1)$ inteiros, exatamente metade deles pertence a $B(a, b)$. Logo,

$$\sharp B(a, b) = \frac{(a-1)(b-1)}{2}.$$

12. Perceba que devemos ter $mdc(a, b) = 1$ pois caso contrário qualquer valor que não fosse múltiplo de $mdc(a, b)$ não seria uma pontuação possível e sabe mos que existe apenas um número finito de tais valores. Em virtude do exercício anterior, $(a-1)(b-1) = 2 \cdot 35 = 70$. Analisemos os possíveis pares de divisores de 70 tendo em mente que $a < b$:

$$\begin{aligned} (a-1)(b-1) &= 1 \cdot 70 \Rightarrow (a, b) = (2, 71) \\ (a-1)(b-1) &= 2 \cdot 35 \Rightarrow (a, b) = (3, 36) \\ (a-1)(b-1) &= 5 \cdot 14 \Rightarrow (a, b) = (6, 15) \\ (a-1)(b-1) &= 7 \cdot 10 \Rightarrow (a, b) = (8, 11) \end{aligned}$$

Não podemos ter $(a, b) = (2, 71)$ pois $58 = 2 \cdot 29$. Excluindo os outros dois casos em que $mdc(a, b) \neq 1$, temos $a = 8$ e $b = 11$.

Produzido por Arquimedes Curso de Ensino
contato@cursoarquimedes.com