Bézout e Outros Bizus

Davi Lopes – Olimpíada Brasileira de Matemática

18ª Semana Olímpica – São José do Rio Preto, SP

1. Introdução

Neste material, iremos demonstrar o teorema de Bézout, que diz que, dados a e b inteiros positivos, existem inteiros x, y tais que:

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

Além disso, mostraremos algumas extensões desse resultado, e mostraremos também como esse teorema é importante para o desenvolvimento da Teoria dos Números, sobretudo na parte relativa à congruências.

2. Um Resultado Preliminar: O Algoritmo de Euclides

Antes de demonstrarmos o teorema de Bézout, precisaremos de um resultado inicial, que, embora conhecido mais pela sua aplicação prática para encontrar o mdc de dois números, sua formulação teórica se mostra formidável para provar a existência dos inteiros x e y. Vejamos então o Algoritmo de Euclides.

Teorema (Algoritmo de Euclides): Dados dois inteiros positivos a, b, considere as divisões sucessivas, onde as letras q são quocientes e as letras r são restos:

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

...

$$r_k = q_{k+1} r_{k+1} + r_{k+2}$$

$$r_{k+1} = q_{k+2} r_{k+2}$$

(Observe que essas divisões sucessivas em algum momento vão acabar, pois do algoritmo da divisão temos $b > r_0 > r_1 > r_2 > \cdots$, e se a sequencia de restos não acabasse, em algum momento teríamos um resto negativo, o que é um absurdo).

Então, $mdc(a, b) = r_{k+2}$ é o último resto não nulo das divisões sucessivas.

Demonstração: Antes de demonstrarmos o resultado do Algoritmo de Euclides, precisaremos de um lema inicial, que é o seguinte:

Lema Útil: Sejam a, b inteiros positivos e $t \in \mathbb{Z}$. Então $mdc(a,b) = mdc(a, b + at)$, e que $mdc(a,b) = mdc(a + bt, b)$

Demonstração: Antes de demonstrarmos o lema útil precisamos saber o que é um mdc, mas aí já é esticar demais! (☺) Então vamos provar nosso lema (que é útil não só para provar o Algoritmo de Euclides, mas para quase tudo que envolva mdc).

Vamos provar que $mdc(a,b) = mdc(a, a + bt)$. Seja $d = mdc(a,b)$ e $d' = mdc(a, b + at)$. Temos que, olhando para $mdc(a,b)$:

$$d|a \text{ e } d|b \Rightarrow d|a, d|at \text{ e } d|b \Rightarrow d|a\ e\ d|b + at$$

Assim, d é um divisor comum de a e $b + at$, e como d' é o maior divisor comum, temos então $d' \geq d$. Agora, olhando para $mdc(a, b + at)$:

$$d'|a \text{ e } d'|b + at \Rightarrow d'|a, d'|at \text{ e } d'|b + at \Rightarrow d'|a \text{ e } d'|b + at - at \Rightarrow d'|a \text{ e } d'|b$$

Assim, d' é um divisor comum de a e b, e como d é o maior divisor comum, temos $d \geq d'$. Ora, já provamos que $d' \geq d$, de modo que $d = d'$, como queríamos. A outra identidade se demonstra de forma completamente análoga.

Com esse lema, fica bem fácil demonstrar o lema de Euclides. Veja só:

$$mdc(a,b) = mdc(a - q_0 b, b) = mdc(r_0, b) \Rightarrow mdc(a,b) = mdc(b, r_0)$$

$$mdc(b, r_0) = mdc(b - q_1 r_0, r_0) = mdc(r_1, r_0) \Rightarrow mdc(b, r_0) = mdc(r_0, r_1)$$

Fazendo isso sucessivamente: $mdc(a,b) = mdc(b, r_0) = mdc(r_0, r_1) = mdc(r_1, r_2) = \cdots = mdc(r_{k+1}, r_{k+2}) = mdc(q_{k+2} r_{k+2}, r_{k+2}) = r_{k+2}$, donde temos que $mdc(a,b) = r_{k+2}$, como queríamos provar ■

3. Demonstrando o Teorema de Bézout

Eis o nosso grande teorema:

Teorema de Bézout: Dados a e b inteiros positivos, existem inteiros x, y tais que:

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

Demonstração: Vamos analisar de novo as divisões sucessivas. Temos que:

$$r_{k+2} = -q_{k+1} r_{k+1} + r_k$$

Agora, $r_{k+1} = -q_k r_k + r_{k-1}$, de modo que, ao substituirmos r_{k+1} na equação acima:

$$r_{k+2} = -q_{k+1}(-q_k r_k + r_{k-1}) + r_k = (q_{k+1} q_k + 1) r_k - q_{k+1} r_{k-1}$$

Chamando $x_k = q_{k+1} q_k + 1$ e $y_k = -q_{k+1}$, temos x_k, y_k inteiros e:

$$r_{k+2} = x_k r_k + y_k r_{k-1}$$

Agora, $r_k = -q_{k-1}r_{k-1} + r_{k-2}$, de modo que, ao substituirmos r_k na equação acima:

$$r_{k+2} = x_k(-q_{k-1}r_{k-1} + r_{k-2}) + y_k r_{k-1} = (-q_{k-1}x_k + y_k)r_{k-1} + x_k r_{k-2}$$

Chamando $x_{k-1} = -q_{k-1}x_k + y_k$ e $y_{k-1} = x_k$, temos x_{k-1}, y_{k-1} inteiros e:

$$r_{k+2} = x_{k-1}r_{k-1} + y_{k-1}r_{k-2}$$

Fazendo isso sucessivamente, chegaremos ao final de tudo que existem inteiros x_1, y_1 tais que:

$$r_{k+2} = x_1 r_1 + y_1 r_0$$

Agora, sendo $r_1 = b - q_1 r_0$ e $r_0 = a - q_0 b$, temos que, ao substituir r_1 e depois r_0:

$$r_{k+2} = x_1(b - q_1 r_0) + y_1 r_0 = (y_1 - x_1 q_1)r_0 + x_1 b = (y_1 - x_1 q_1)(a - q_0 b) + x_1 b =$$

$$= a(y_1 - x_1 q_1) + b(-q_0 y_1 + x_1 q_0 q_1 + x_1)$$

Chamando $x = y_1 - x_1 q_1$ e $y = -q_0 y_1 + x_1 q_0 q_1 + x_1$, temos que x, y são inteiros e como $r_{k+2} = mdc(a,b)$, segue que $mdc(a,b) = ax + by$, mostrando assim a existência de x, y inteiros ■

Observação 1: Observe que com os artifícios dessa demonstração é possível encontrar x e y, bastando para isso encontrar x_k, y_k, depois x_{k-1}, y_{k-1} e assim por diante.

Observação 2: Observe ainda que todo múltiplo de $mdc(a,b)$ pode ser escrito na forma $ax + by$. Com efeito, se $M = k.mdc(a,b)$ é um múltiplo, então $M = k(ax + by) = a(kx) + b(ky)$. Além disso, todos os números da forma $ax + by$, com $x, y \in \mathbb{Z}$, são múltiplos de $mdc(a,b)$, pois a e b são múltiplos também.

Resumindo, o conjunto dos números da forma $ax + by$, onde x, y podem variar sobre todos os inteiros, é exatamente o conjunto dos múltiplos de $mdc(a,b)$.

Observação 3: Existe outra demonstração do Teorema de Bézout, sem usar o algoritmo de Euclides. Veja:

Para cada par (x, y), associemos o número $n(x,y) = ax + by$, e seja *N* o conjunto de todos esses números, ou seja, $N = \{n(x,y) | x, y \in \mathbb{Z}\}$. Note que *N* é um conjunto não vazio (afinal, $n(1,0) = a.1 + b.0 = a$, $n(0,1) = a.0 + b.1 = b$, $n(a,b) = a.a + b.b = a^2 + b^2$, etc., estão todos em *N*). Além disso, não é difícil ver que ele possui infinitos elementos positivos e infinitos elementos negativos. Com isso, se consideramos os elementos positivos, existe um deles que é o menor de todos. Seja $n(x_0, y_0) = c$ esse elemento mínimo. Provaremos que $c|a$ e $c|b$.

Suponha que $c \nmid a$. Assim, pelo algoritmo da divisão, existem $q, r \in \mathbb{N}$ tais que $a = qc + r$ e $0 < r < c$ (Note que $r = 0$ não é possível, pois aí $c|a$). Mas sabemos que:

$$c = n(x_0, y_0) = ax_0 + by_0 \Rightarrow a = qc + r = q(ax_0 + by_0) + r \Rightarrow$$

$$\Rightarrow r = a - q(ax_0 + by_0) = a\,\underbrace{(1 - qx_0)}_{x_1} + b\,\underbrace{(-qy_0)}_{y_1} \Rightarrow r = ax_1 + by_1 = n(x_1, y_1)$$

Com isso, temos que $r = n(x_1, y_1)$ é inteiro positivo, e $r \in N$. Daí, ele é maior do que ou igual ao mínimo, que é *c*. Então, $r \geq c$. Mas, do algoritmo da divisão, $r < c$, um absurdo.

Com isso, concluímos que $c|a$ e, analogamente, $c|b$. Assim, *c* é um divisor comum, e como $d = mdc(a, b)$ é o máximo divisor comum de *a* e *b*, temos $c \leq d$.

Agora, temos que:

$$\frac{c}{d} = \frac{a}{d}.x_0 + \frac{b}{d}.y_0$$

É inteiro, uma vez que $\frac{a}{d}, \frac{b}{d}, x_0, y_0$ são inteiros. Com isso, temos que $d|c$, donde $c \geq d$ (*c, d* são todos positivos). Juntando isso ao fato de que $c \leq d$, temos $c = d$. Portanto, $d = n(x_0, y_0 = ax_0 + by_0$ é o número procurado para ser $mdc(a, b)$ ■

4. Uns Problemas Interessantes

4.1. Breve Historinha

Agora vamos dar uma breve pausa nas contas e vejamos uma historinha baseada em fatos reais que, por incrível que pareça, tem tudo a ver com o que estamos vendo aqui.

Certa vez, um matemático brasileiro estava na Argentina, participando de uma olimpíada de matemática como jurado. Quando todos os jurados estavam jantando, a televisão do restaurante onde eles estavam estava mostrando uma partida de um esporte bem diferente dos brasileiros: rúgbi. O matemático brasileiro, querendo se informar sobre como o jogo funcionava, perguntou a uma amiga argentina, também uma matemática:

- Esse jogo, que você disse ser rúgbi, como ele funciona?

- Ah... não sei muito bem, mas você pode fazer 3 ou 5 pontos, dependendo da posição onde você faça o gol, eu acho. Mas uma coisa eu sei!

- O que?

- Nesse jogo não dá pra perder de 7 a 1. Acho que vocês brasileiros vão gostar dele!

Todos ali riram do brasileiro e nesse momento ele percebeu duas coisas: a primeira era que a vergonha que o Brasil passou na copa era tão grande que o mundo todo (literalmente!) iria mangar por muito tempo (e os argentinos mais ainda... ah, esses argentinos!). A outra é que tanto 1 como 7 não podem ser escritos na forma $3x + 5y$, onde x, y são inteiros não-negativos.

Como $mdc(3,5) = 1$, sabemos que, pelo teorema de Bézout, que todo inteiro pode ser escrito sob a forma $3x + 5y$, onde $x, y \in \mathbb{Z}$ (inclusive $1 = 3.2 + 5.(-1)$ e $7 = 3.4 + 5.(-1)$), mas... e se precisássemos que x, y fossem não-negativos, como no caso do jogo de rúgbi, onde não se pode fazer pontuações negativas? Vendo sob essa ótica, percebemos que é interessante saber quais são os inteiros que podem ser escritos sob a forma $3x + 5y$, com $x, y \geq 0$ inteiros.

De um modo mais geral, dados a, b inteiros positivos, com $mdc(a, b) = 1$:

- Quando $n \geq 0$ inteiro pode ser escrito na forma $ax + by$, com $x, y \geq 0$ inteiros?
- Será que a partir de certo valor C, todo $n \geq C$ pode ser escrito assim?
- Quantos $n \geq 0$ não podem ser escritos assim?

4.2. Respondendo à Primeira Pergunta

Vamos analisar o problema de um modo mais geral: dados a, b inteiros positivos com $mdc(a, b) = 1$ e um inteiro não-negativo n, é possível escrever $n = ax + by$, com x, y inteiros não-negativos? A resposta é: depende do valor de n. Mas como é essa dependência? Para responder a isso, recorreremos ao teorema de Bézout.

Primeiro, façamos uma breve observação: considere inteiros x_0, y_0, x_1, y_1 tais que $n = ax_0 + by_0 = ax_1 + by_1$ (eles existem pela observação 2 do teorema de Bézout, pois $mdc(a, b) = 1$). Sabemos que:

$$b|0 \Rightarrow b|ax_0 + by_0 - (ax_1 + by_1) \Rightarrow b|a(x_0 - x_1) + b(y_0 - y_1) \Rightarrow$$

$$\Rightarrow b|a(x_0 - x_1) \Rightarrow b|x_0 - x_1$$

Note que na última passagem usamos que $mdc(a, b) = 1$ para "tirar" o a da divisibilidade. Como $b|x_0 - x_1$, temos que x_0, x_1 deixam mesmo resto na divisão por b. Analogamente, temos que y_0, y_1 deixam mesmo resto na divisão por a.

Outra observação bem sagaz é que, ao escrevermos $n = ax_0 + by_0 = a(x_0 + kb) + b(y_0 - ka)$ e variarmos o valor de k nos inteiros, percebemos que todo número que deixa o mesmo resto que x_0 na divisão por b pode assumir o papel de x na equação de Bézout, $n = ax + by$, e todo número que deixa o mesmo resto que y_0 na divisão por a pode assumir o papel de y na equação.

Dessa forma, vemos que, embora a equação $n = ax + by$ não tenha solução única (x, y) (há infinitas soluções), elas são "quase" únicas, no sentido de que o resto de x por b e o resto de y por a são únicos.

Agora estamos prontos para responder nossa pergunta: para saber se n pode ser escrito na forma $ax + by$, com $x, y \geq 0$ inteiros, considere $n = ax_0 + by_0$ (x_0, y_0 inteiros, positivos ou não) e seja r o resto que x deixa por b (sabemos que r é o mesmo qualquer que seja o x_0 escolhido). Agora, escreva $n = ar + by_1$. Se $y_1 \geq 0$, n pode ser escrito na forma (a própria forma $n = ar + by_1$ já satisfaz à questão, pois $r, y_1 \geq 0$); se $y_1 < 0$, então n não pode ser escrito na forma, pois caso $n = ar + by_1 = ax + by$, com $x, y \geq 0$, então, como x é não-negativo e deixa resto r por b, temos que $x \geq r$, donde $ar - ax \leq 0 \Rightarrow by - by_1 \leq 0 \Rightarrow y_1 \leq y < 0 \Rightarrow y_1 < 0$, uma contradição.

Portanto, no nosso exemplo do jogo de Rúgbi, é impossível obter 1,2,4 e 7 pontos, pois:

$1 = 3.(2) + 5.(-1)$; $2 = 3.(4) + 5.(-2)$; $4 = 3.(3) + 5.(-1)$; $7 = 3.(4) + 5.(-1)$

Por outro lado, é possível obter 3,5,6,8 pontos, pois:

$3 = 3.(1) + 5.0$; $5 = 3.(0) + 5.(1)$; $6 = 3.(2) + 5.(0)$; $8 = 3.(1) + 5.(1)$

Observe que os números que acompanham o 3 na multiplicação são sempre números entre 0 e 4, ou seja, restos na divisão por 5.

Frequentemente, escreveremos $n = ax + by$ com $x, y \in \mathbb{Z}$ e $0 \leq x \leq b - 1$, pois é útil tomarmos a primeira variável como sendo o resto da divisão por b, de modo a podermos analisar se n se encaixa ou não no que queremos (se você é um "x-fóbico", você também pode tomar y como sendo o resto da divisão por a, pois a ideia é análoga).

4.3. Respondendo à Segunda Pergunta

Existe um inteiro para o qual todo inteiro a partir dele pode ser expresso como $ax + by$, $x, y \geq 0$? A resposta é sim, e o que é melhor: a melhor cota para esse número é exatamente $(a-1)(b-1)$. Vamos lá ver porque?

Primeiramente, escreva $n = ax + by$, com x, y inteiros e $0 \leq x \leq b - 1$ (já vimos que podemos sempre fazer isso). A questão que deve ser respondida é a seguinte: será que $n \geq (a-1)(b-1)$ implica $y \geq 0$? Vejamos.

Suponha que $y < 0$. Daí, $y \leq -1$, donde:

$$n = ax + by \leq a(b-1) + b(-1) = ab - a - b < (a-1)(b-1)$$

O que é um absurdo. Logo, todo número a partir de $(a-1)(b-1)$ pode ser escrito conforme a gente quer, de modo que só há um número finito de inteiros não negativos para o qual é impossível escrever como $ax + by$, $x, y \geq 0$ inteiros (em particular, num jogo de Rúgbi, toda pontuação a partir de $(3-1)(5-1) = 8$ pode ser obtida). A última pergunta que fica é a seguinte: para quantos inteiros é impossível?

4.4. Respondendo à Terceira Pergunta

Para responder à terceira pergunta, considere N como sendo o conjunto de todos os inteiros entre 0 e $2ab - a - b$ (ou seja, $N = \{0,1,2, \dots, 2ab - a - b\}$). Observe que se tomarmos n um elemento qualquer de N, e escrevermos $n = ax + by$, com $0 \leq x < b$, então poderemos ter $y < 0$, ou $0 \leq y < a$ ou $a \leq y < 2a - 1$ ($y \geq 2b - 1$ é impossível, pois aí $n = ax + by \geq by \geq b(2a-1) > 2ab - a - b$, absurdo). Então, o conjunto N pode ser dividido em 3 subconjuntos disjuntos, a saber:

$$N_1 = \{n \in N | n = ax + by, \text{com } 0 \leq x < b \text{ e } y < 0\}$$

$$N_2 = \{n \in N | n = ax + by, \text{com } 0 \leq x < b \text{ e } 0 \leq y < a\}$$

$$N_3 = \{n \in N | n = ax + by, \text{com } 0 \leq x < b \text{ e } a \leq y < 2a - 1\}$$

Queremos saber quantos elementos tem o conjunto N_1, pois todos os números que não podem ser escritos como desejamos estão entre 0 e $2ab - a - b$ (já que $2ab - a - b > (a-1)(b-1)$). Temos também que $|N_1| + |N_2| + |N_3| = |N| = 2ab - a - b + 1$, onde $|A|$ representa a quantidade de elementos de A.

Olhando para os elementos de N_2, vemos que cada escolha de x e y dá um número diferente, uma vez que as escolhas são justamente sobre os restos que x e y deixam por b e a, respectivamente, e sabemos que restos diferentes implicam números diferentes. Além disso, $0 \leq a(0) + b(0) \leq ax + by \leq a(b-1) + b(a-1) = 2ab - a - b$, de modo que cada escolha de x e y gera um número que está no conjunto N. Portanto, como temos b modos de escolher x e a modos de escolher y, então N_2 possui ab elementos.

Daí, temos que $|N_1| + ab + |N_3| = 2ab - a - b + 1 \Rightarrow |N_1| + |N_3| = (a-1)(b-1)$. Provaremos agora que N_1 e N_3 possuem a mesma quantidade de elementos, provando que $n \in N_1$ se, e somente se $2ab - a - b - n \in N_3$. Com isso, associamos a cada elemento de N_1 um elemento de N_3 e vice-versa ($n \leftrightarrow 2ab - a - b - n$), o que prova que $|N_1| = |N_3|$.

Temos $n \in N_1$ se, e somente se $n = ax + by$, com $0 \leq x < b$ e $-a < y \leq -1$ (observe que, de fato, $y > -a$, pois se $y \leq -a$, do fato de que $x < b$, teríamos $n = ax + by < ab - ab = 0 \Rightarrow n < 0$, contradição). Assim, como:

$$n' = 2ab - a - b - n = a(b - 1 - x) + b(a - 1 - y) = ax' + by'$$

(onde $x' = b - 1 - x$ e $y' = b - 1 - y$), temos que $0 \leq x < b$ e $-a < y < 0$ se, e somente se $0 \leq x' < b$ e $a \leq y' < 2a - 1$. Isso significa que $n \in N_1$ se, e somente se, $n' \in N_3$. Com isso, fica demonstrada que nossa correspondência é biunívoca.

Finalmente, de $|N_1| = |N_3|$ e de $|N_1| + |N_3| = (a-1)(b-1)$, temos que $|N_1| = \frac{(a-1)(b-1)}{2}$, ou seja, há $\frac{(a-1)(b-1)}{2}$ inteiros não-negativos que não podem ser escritos sob a forma $ax + by$, com $x, y \geq 0$ inteiros. No caso do jogo de Rúgbi, há $\frac{(3-1)(5-1)}{2} = 4$ inteiros, que já sabemos quem são: 1, 2, 4 e 7.

5. Outros Bizus

O Teorema de Bézout é importantíssimo no estudo da Teoria dos Números, pois é a partir dele que conseguimos deduzir outros "bizus". Um deles está relacionado com inversos multiplicativos módulo um natural.

Teorema: Seja n um inteiro positivo e seja a um inteiro tal que $mdc(a,n) = 1$. Então, existe $x \in \mathbb{Z}$ tal que $ax \equiv 1\ (mod.n)$. Além disso, o valor de x é único módulo n.

Prova: Pelo teorema de Bézout, existem inteiros x, y tais que $ax + ny = mdc(a,n) = 1 \Rightarrow ax = 1 - ny \equiv 1 - 0 \equiv 1\ (mod.n)$. Logo, o valor de x do Teorema de Bézout é um possível inverso multiplicativo, mostrando que inversos multiplicativos de fato existem.

Para provarmos que x e único módulo n, basta provar que $ax \equiv ax'(mod.n)$ implica $x \equiv x'(mod.n)$. Isso decorre diretamente do fato de que podemos "cortar" termos primos com o módulo, mas para provar esse fato, precisaremos mais uma vez do bizu d Bézout! Se você gostou do trocadilho, veja abaixo; senão, também veja abaixo!

Observe que $ax \equiv ax'(mod.n) \Rightarrow n|a(x - x')$. Ora, pelo teorema de Bézout, existem inteiros y, z tais que $ay + nz = 1 \Rightarrow ay = 1 - nz$. Daí, como $n|a(x - x') \Rightarrow n|ay(x - x') \Rightarrow n|(1 - nz)(x - x') \Rightarrow n|x - x'$, demonstrando que $x \equiv x'\ (mod.n)$, encerrando a demonstração ■

Devido à existência e unicidade desse inverso multiplicativo, podemos chama-lo de a^{-1}. Apesar de que a^{-1} seja um número inteiro (e, portanto, não seja a fração $\frac{1}{a}$), nas congruências podemos muitas vezes trocar frações por inversos multiplicativos! Esse bizu, combinado com alguns outros (como binômio de Newton e Raízes primitivas) é extremamente eficiente para se resolver problemas bem difíceis, como o teorema de Wolstenholme e o problema 3 da Ibero-americana de Matemática de 2005.

Além disso, o inverso multiplicativo serve também para demonstrar outros três teoremas extremamente úteis em teoria dos números. São eles:

Teorema de Wilson: Seja p um número primo. Então, $(p-1)! \equiv -1\ (mod.p)$

Teorema de Fermat: Seja p um primo, $n \in \mathbb{N}$ e $a \in \mathbb{Z}$. Então, $a^p \equiv a\ (mod.p)$

Teorema de Euler: Sejam a, n inteiros positivos com $mdc(a,n) = 1$. Então, $a^{\varphi(n)} \equiv 1\ (mod.n)$, onde $\varphi(n)$ é a quantidade de inteiros entre 1 e n que são relativamente primos com n.

Fica como exercício para você, amigo leitor, demostrar essas propriedades. Se estiver tendo dificuldade em demonstrar alguma delas, não se preocupe: a maioria dos livros de teoria elementar dos números enuncia e prova esses teoremas, pois eles são extremamente importantes!

Bom, chega de teoria (não de teoria dos números! :p), e vamos à prática!

6. Exercícios

Problema 1: Encontre todas as soluções inteiras de cada uma das equações:

(a) $2x + 3y = 5$

(b) $5x + 3y = 7$
(c) $21x + 48y = 6$
(d) $147x + 258y = 369$
(e) $2x + 3y + 4z = 5$
(f) $2x + 3y + 5z = 11$

Problema 2: Demonstrar que se $a, b, c, d, m, n > 0$ são inteiros tais que $ad - bc = 1$, então $mdc(am + bn, cm + dn) = mdc(m, n)$.

Problema 3: (a) Demonstre que $mdc(2^a - 1, 2^b - 1) = 2^{mdc(a,b)} - 1$.

(b) Demonstre que se $x > y$, então $mdc(x^a - y^a, x^b - y^b) = x^{mdc(a,b)} - y^{mdc(a,b)}$.

Problema 4: Sejam a, b inteiros positivos primos entre si. Prove que não existem inteiros não-negativos x, y tais que $ab - a - b = ax + by$. Com isso, prove que $(a - 1)(b - 1)$ é o menor valor possível de C tal que todo inteiro maior do que ou igual a C pode ser escrito na forma $ax + by$, com x, y inteiros não-negativos.

Problema 5 (OBM/2014): Encontre todos os inteiros n, $n > 1$, com a seguinte propriedade: para todo k, $0 \leq k < n$, existe um múltiplo de n cuja soma dos algarismos, na base decimal, deixa resto k na divisão por n.

Problema 6 (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 7: (a) Em Gugulândia, o jogo de basquete é jogado com regras diferentes. Existem apenas dois tipo de pontuações para as cestas: 5 e 11 pontos. É possível um time fazer 39 pontos em uma partida?

(b) Suponha agora que as pontuações das cestas do basquete de Gugulândia 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.

Problema 8 (AMC/1989): Seja n um inteiro positivo. Se a equação $2x + 2y + z = n$ tem 28 soluções inteiras positivas (x, y, z), determine todos os possíveis valores de n.

Problema 9 (MOSP/2005): Em cada vértice de um cubo, um inteiro está escrito. Uma *transição legal* no cubo consiste em pegar qualquer vértice do cubo e adicionar o valor escrito naquele vértice em algum vértice adjacente (isto é, pegue um vértice com algum valor x escrito nele, um vértice adjacente com algum valor y escrito nele, e troque y por $y + x$). Prove que existe uma sequência finita de transições legais tais que, no fim, todos os 8 números escritos mesmo resto por 2005.

Problema 10 (IMO1983): 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 $abx + bcy + caz$, onde x, y, z são inteiros não negativos.