Teorema de Bézout

Alessandro Machado

1 Introdução

1.1 Contextualização

Ao trabalharmos com divisibilidade e seus fatores primos, sentimos a nescessidade de estabelecer uma relação numérica mais formal entre números, para que assim podemos conseguir mais informação ao reescrevelos separando o que relaciona-os e o que não. Por exemplo, se temos que $5|45$, isto é $5|3 \cdot 15$, percebemos intuitivamente que o 3 não contribui para essa divisibilidade, enquanto 15 tem todos os "fatores" 5 que precisamos, outro exemplo seria $5^2|10 \cdot 15 = 2 \cdot 5 \cdot 5 \cdot 3$, então nesse caso ignoraremos o 2 e 3 porque eles não se "relacionam" com 5, ficando com $5^2|5^2$, que ainda é verdade.

1.2 Esclarecimentos

Quando nos referimos a essa relação (que definiremos mais a frente), há duas formas de usá-la. Uma delas é perceber que cada número pode ser escrito unicamente em fatoração de números primos, interpretando essa relação como se fosse a "interseção" dessas fatorações (que já foi coberta em um material anterior). Enquanto a que veremos nesse material se trata da aplicação de um teorema muito poderoso para essa relação que é o *Teorema de Bézout* (uma forma de reescrever essa relação que veremos posteriormente).

---

2 Definições

2.1 Máximo divisor comum

Denotamos por $mdc(a, b) = d \iff d|a, d|b$ e $\forall\ d'$ tal que $d'|a, d'|b \implies d' \leq d$. Isto é, $mdc(a, b)$ é o maior divisor comum de a e b.

Note que $mdc(a, b) = mdc(b, a) = mdc(a, -b) \geq 1$, logo apenas analisamos $a, b \in \mathbb{N}$ por simplicidade. Também vale observar que $n|0\ \forall\ n \in \mathbb{Z}$, ou seja, $mdc(a, 0) = a$, pois $a|a$ e $a|0$, entretanto $mdc(0, 0)$ é indeterminado, pois qualquer inteiro divide 0.

. . . . . .

2.2 Teorema de Bézout

Teorema

Sejam $a, b \in \mathbb{Z}_*$, então existem $x, y \in \mathbb{Z}$ tais que $ax + by = d \iff mdc(a, b)|d$.

Prova. Primeiro provaremos a ida. Note que $mdc(a,b)|a$ e $mdc(a,b)|b \implies mdc(a,b)|ax+by=d$ $\square$

Agora, mostraremos que todo multiplo de $mdc(a,b)$ pode ser escrito como $ax+by$ (a volta). Defina $v(x,y)=ax+by$ e o conjunto $V=\{v(x,y) \mid x,y \in \mathbb{Z}\}$, então tome (x_0,y_0) para serem tais que $v(x_0,y_0)$ seja o menor inteiro positivo no conjunto (por *Princípio da Boa Ordem*).

Queremos provar que $v(x_0,y_0)=c=ax_0+by_0$ divide a e b. Suponha que $c \nmid a$ logo, por *Algoritmo da Divisão* temos que $a=qc+r, 0<r<c$ ($r \neq 0$ pois $c \nmid a$), então $a=qc+r=q(ax_0+by_0)+r \implies r=a-q(ax_0+by_0)=a(1-qx_0)+b(-qy_0)=v(1-qx_0,-qy_0) \in V$, mas perceba que $0<r<c$ e $r \in V$, absurdo pois tomamos c para ser o menor elemento positivo de V! Logo, $c|a$ e $c|b \implies c \leq mdc(a,b)$ pela definição, pois todo divisor comum de a e b é menor ou igual ao seu máximo divisor comum. Porém, perceba que $mdc(a,b)|a$ e $mdc(a,b)|b \implies mdc(a,b)|ax_0+b_0=c \implies mdc(a,b) \leq c$, então $c=mdc(a,b)$, portanto é possível escrever o $mdc(a,b)$ como $ax+by$.

Mas, como $mdc(a,b)|d \implies d=d'mdc(a,b)$. Então, tendo $v(x_0,y_0)=ax_0+by_0=mdc(a,b) \implies d'v(x_0,y_0)=d'ax_0+d'by_0=a(d'x_0)+b(d'y_0)=v(d'x_0,d'y_0)=d' \cdot mdc(a,b)=d$, portanto podemos escrever qualquer d múltiplo de $mdc(a,b)$ também $\blacksquare$

3 Corolário

3.1 Comentário

O *Teorema de Bézout* que acabamos de ver é uma ferramenta muito forte em *Teoria dos Números*, ela nos permite provar muitas propriedades e teoremas de forma muito resumida e muitas vezes, com apenas uma única aplicação direta (ou nem tanto) do teorema.

O objetivo desse material é treiná-los a identificar quando e de que forma aplicar o *Teorema de Bézout* pois ele, por si só, é um teorema simples, o difícil é identificar sua aplicação.

3.2 Propriedades

.....

Propriedade 1.

Se d é um divisor comum de a e b (ou seja, $d|a, d|b$), então d divide o $mdc(a,b)$.

Prova. Sabemos que se $d|a$ e $d|b$, então <u>d divide qualquer combinação linear de a e b</u> (isto é, $ax+by$, $\forall\ x,y \in \mathbb{Z}$), e queremos que $d|mdc(a,b)$, isso nos motiva a escrever

$mdc(a,b)$ como uma combinação linear de a e b.

Então, por *Teorema de Bézout*, existem $x, y \in \mathbb{Z}$ tais que $mdc(a,b) = ax + by$. Como $d|a \implies d|ax$ e $d|b \implies d|by \implies d|ax + by = mdc(a,b)$ ■

. . . . . .

Propriedade 2.

Se c é um inteiro positivo, então $mdc(ca, cb) = c \cdot mdc(a,b)$.

Prova. Para isso, usaremos uma ideia recorrente quando queremos uma igualdade trabalhando apenas com divisibilidade. Isto é, provaremos que os dois se dividem, ou seja, $mdc(ca,cb)|c \cdot mdc(a,b)$ e que $c \cdot mdc(a,b)|mdc(ca,cb)$, pois assim, se $m|n \implies |m| \leq |n|$ e $n|m \implies |n| \leq |m|$, logo $|m| = |n|$ (mas como $mdc(k,l) > 0$, podemos retirar o módulo).

Inicialmente, provaremos que $\boxed{mdc(ca,cb)|c \cdot mdc(a,b)}$, sendo que a única coisa que sabemos é que $mdc(ca,cb)|ca$ e $mdc(ca,cb)|cb$, ou seja, que $mdc(ca,cb)$ divide qualquer combinação linear de ca e cb e queremos obter que $mdc(ca,cb)|c \cdot mdc(a,b)$, então isso nos motiva a escrevermos $c \cdot mdc(a,b)$ como uma combinação linear de ca e cb, que é o mesmo que escrevermos apenas $mdc(a,b)$ como uma combinação linear de a e b (que é o que o *Teorema de Bézout* afirma).

Então, por *Teorema de Bézout* existem $x_0, y_0 \in \mathbb{Z}$ tais que $mdc(a,b) = ax_0 + by_0$. Sabemos que $mdc(ca,cb)|ca \implies mdc(ca,cb)|cax_0$ e $mdc(ca,cb)|cb \implies mdc(ca,cb)|cby_0 \implies mdc(ca,cb)|cax_0 + cby_0 = c(ax_0 + by_0) = c \cdot mdc(a,b)$ □

Agora provaremos que $\boxed{c \cdot mdc(a,b)|mdc(ca,cb)}$ com um raciocínio análogo, pois sabemos que $mdc(a,b)|a \implies c \cdot mdc(a,b)|ca$ e $mdc(a,b)|b \implies c \cdot mdc(a,b)|cb$.

Para isso temos que existem $x_1, y_1 \in \mathbb{Z}$ tais que $mdc(ca,cb) = (ca)x_1 + (cb)y_1$ por *Teorema de Bézout*. Como temos que $mdc(a,b)|a \implies c \cdot mdc(a,b)|ca \implies c \cdot mdc(a,b)|cax_1$ e $mdc(a,b)|b \implies c \cdot mdc(a,b)|cb \implies c \cdot mdc(a,b)|cby_1 \implies c \cdot mdc(a,b)|(ca)x_1 + (cb)y_1 = mdc(ca,cb) \implies mdc(ca,cb) = c \cdot mdc(a,b)$ ■

. . . . . .

Propriedade 3.

Se a, b e c são inteiros não nulos tais que $a|bc$ então $\dfrac{a}{mdc(a,b)}|c$.

Prova. Primeiramente, simplificaremos o problema para uma versão mais simples apenas dividindo pelos fatores em comum, isto é, se $mdc(a,b) = 1$, então o problema seria $a|bc \implies a|c$, para isso usaremos um truque muito útil na maioria dos problemas de *Teoria dos Números*, que é, reescrever a em termos de $mdc(a,b)$ multiplicado por uma variável a_0, pois assim conseguiremos dividir essa divisibilidade por $mdc(a,b)$ de ambos

os lados

Chame $mdc(a,b) = d$ e como $d|a$ e $d|b$, escreva-os como $a = da_0$ e $b = db_0$, sabemos que $mdc(a,b) = mdc(da_0, db_0) = d \cdot mdc(a_0, b_0) \implies mdc(a_0, b_0) = \dfrac{mdc(a,b)}{d} = 1$. E, temos que $a|bc \implies da_0|db_0c \implies a_0|b_0c$. Agora, por *Teorema de Bézout*, existem $x, y \in \mathbb{Z}$ tais que $c = c \cdot mdc(a_0, b_0) = mdc(ca_0, cb_0) = (ca_0)x + (cb_0)y$, sendo que $a_0|b_0c \implies a_0|b_0cy$ e $a_0|ca_0x \implies a_0|(ca_0)x + (cb_0)y = c \implies a_0 = \dfrac{a}{mdc(a,b)}|c$ ■

. . . . . .

Propriedade 4.

Se $a, b, k, n \in \mathbb{Z}$ tais que $ka \equiv kb \pmod{n}$, então $a \equiv b \pmod{\dfrac{n}{mdc(n,k)}}$.

Prova. Isso é uma consequência direta da propriedade anterior, porém muito útil, principalmente quando $mdc(k,n) = 1$. Pois $ka \equiv kb \pmod{n} \iff n|ka - kb = k(a-b)$, mas aplicando a propriedade anterior, temos que $\dfrac{n}{mdc(n,k)}|a - b \iff a \equiv b \pmod{\dfrac{n}{mdc(n,k)}}$ ■

. . . . . .

Propriedade 5.

Se $a, n \in \mathbb{N}$ e $mdc(a,n) = 1$, existe um único b módulo n tal que $ab \equiv 1 \pmod{n}$. Tal b é chamado de inverso multiplicativo de a módulo n, ou representado por a^{-1}.

Prova. Precisaremos provar que tal existe e, também que é único módulo n, ou seja, se $ac \equiv 1 \pmod{n}$, então $b \equiv c \pmod{n}$. Provaremos que existe primeiramente, depois que é único.

Note que existe b tal que $ab \equiv 1 \pmod{n} \iff n|ab - 1 \iff \exists k \in \mathbb{Z}|nk = ab - 1 \iff ab - nk = 1 \iff mdc(a,n) = 1$ o que é verdade. Mas não só isso, note que é um se e somente se, ou seja, se $mdc(a,n) > 1$, tal b não existe! Então tal b existe (note que se $c \equiv b \pmod{n}$, então $ac \equiv ab \equiv 1 \pmod{n}$) □

Agora, suponha que existe $c \not\equiv b \pmod{n}$ onde $ac \equiv 1 \pmod{n}$. Mas, $ab \equiv 1 \pmod{n} \implies ac \equiv 1 \equiv ab \pmod{n}$, porém $mdc(a,n) = 1 \implies c \equiv b \pmod{n}$ (pela propriedade anterior) ■

3.3 Exemplos

. . . . . .

Exemplo 1.

Sejam $a, n, x, y \in \mathbb{Z}$ tais que $a^x \equiv 1 \pmod{n}$ e $a^y \equiv 1 \pmod{n}$, então prove que $a^{mdc(x,y)} \equiv 1 \pmod{n}$.

Solução. Por *Teorema de Bézout*, reescreva $mdc(x, y) = xk + yl$, então $a^{mdc(x,y)} = a^{xk+yl} = a^{xk}a^{yl} = (a^x)^k(a^y)^l \equiv 1^k 1^l \equiv 1 \pmod{n}$, isso é verdade pois, se k for negativo, podemos considerar $(a^{-1})^{-xk}$, pois $ab \equiv 1 \pmod{n} \implies a^k b^k \equiv 1^k \equiv 1 \pmod{n}$ ■

Exemplo 2.

Sejam $a, x, y \in \mathbb{N}$, prove que $mdc(a^x - 1, a^y - 1) = a^{mdc(x,y)} - 1$.

Solução. Para isso, utilizaremos uma técnica muito poderosa em *Teoria dos Números*, que é, provar que $mdc(a^x - 1, a^y - 1)|a^{mdc(x,y)} - 1$ e que $a^{mdc(x,y)} - 1|mdc(a^x - 1, a^y - 1)$, pois assim teremos que $mdc(a^x - 1, a^y - 1)$, uma vez que são positivos.

Note que $mdc(a^x - 1, a^y - 1)|a^{mdc(x,y)} - 1$ é consequência do exemplo anterior, pois chame $d = mdc(a^x - 1, a^y - 1)$, então $a^x \equiv 1 \pmod{d}$ e $a^y \equiv 1 \pmod{d} \implies a^{mdc(x,y)} \equiv 1 \pmod{d} \implies mdc(a^x - 1, a^y - 1)|a^{mdc(x,y)-1}$.

Sendo que se $k|l \implies a^k - 1|a^l - 1$, pois chamando $l = kl'$ temos que $a^k \equiv 1 \pmod{a^k - 1} \implies (a^k)^{l'} = a^l \equiv 1^{l'} = 1 \pmod{a^k - 1} \implies a^k - 1|a^l - 1$. Então, como $d|x$ e $d|y \implies a^d - 1|a^x - 1$ e $a^d - 1|a^y - 1 \implies a^{mdc(x,y)} - 1|mdc(a^x - 1, a^y - 1)$ ■

Exemplo 3.

Mostre que se a, b e c são inteiros tais que $mdc(a, c) = mdc(b, c) = 1$, então $mdc(ab, c) = 1$.

Solução. Existem duas formas de resolver esse problema. A primeira delas é bem comum em problemas na qual queremos provar que dois inteiros não possuem fatores em comum (mdc deles igual a 1), que é provar que não existe um primo que divide ambos. Pois assim, se não há primos que divide ambos, eles não possuem divisores em comum e, divisibilidade com primos é sempre mais fácil.

Já a segunda forma é, usar a informação de $mdc(a, c) = mdc(b, c) = 1$ e reescrevê-la com *Teorema de Bézout*, pois assim podemos manipulá-la para chegarmos que $mdc(ab, c) = 1$.

(*Solução 1.*) Suponha que $mdc(ab, c) > 1$, logo existe um primo p que divide $mdc(ab, c) \implies p|ab$ e $p|c$, sendo que se $p|ab$, então $p|a$ ou $p|b$ (caso contrário, $mdc(a, p) = mdc(b, p) = 1 \implies p|1$). Suponha, sem perder a generalidade, que $p|a \implies p|mdc(a, c) = 1$, pois $p|c$ também, absurdo! Então $mdc(ab, c) = 1$ ■

(*Solução 2.*) Temos que $mdc(a, c) = 1$ então, por *Teorema de Bézout* existem k e l inteiros tais que $ak + cl = 1$, analogamente existem m e n inteiros tais que $bm + cn = 1$, pois $mdc(b, c) = 1$. Multiplicando as equações, obtemos: $(ak + cl)(bm + cn) = 1 \implies (km)ab + (akn + blm + cln)c = 1 \implies mdc(ab, c) = 1$ ■

---

4 Problemas

. . . . . .

Problema 1.

Prove que para todos os x e y inteiros positivos, existe N tal que para todo $n > N$ existem inteiros positivos a e b na qual $ax + by = n \cdot mdc(a, b)$.

. . . . . .

Problema 2. *(PUTNAM 2000)*

Prove que a expressão

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

É um inteiro para todos os pares de inteiros $n \geq m \geq 1$.

. . . . . .

Problema 3. *(Iran 3rd round 2017 Numbers theory final exam P1)*

Sejam x e y inteiros e p um número primo. Suponha que existem m e n inteiros positivos coprimos tais que

$$x^m \equiv y^n \pmod{p}$$

Prove que existe um único inteiro z módulo p tal que

$$x \equiv z^n \pmod{p} \text{ e } y \equiv z^m \pmod{p}$$

. . . . . .

Problema 4. *(IMO Shortlist 2012)*

Chame de A um conjunto admissível de inteiros que tem 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 não-nulos tais que o único conjunto admissível contendo ambos m e n é o conjunto de todos os inteiros.

. . . . . .

Problema 5. *(OBM 2019)*

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) $a_1, a_2, \ldots, a_n$ tais que

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

. . . . . .

4.1 Conclusão

Teorema de Bézout é uma ideia um pouco específica em *Teoria dos Números*, mas mesmo assim muito utilizada. Porém, na maior parte dos problemas e teoremas, ele está presente, mas geralmente como alguma de suas implicações, principalmente em divisibilidade.

A lição mais importante desse material é mostrar na prática como e quando aplicamos *Teorema de Bézout*. Pois muitas vezes, a dificuldade desse tipo de problema é perceber sobre o que se trata, por isso que, se tal problema está relacionado de alguma forma com o *mdc*, temos que considerar de alguma forma o *Teorema de Bézout*.

5 Bibliografia

- **Modern Olympiad Number Theory, Aditya Khurmi**

"A Matemática não mente. Mente quem faz mau uso dela."
–Albert Einstein