Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 3

MDC, MMC, Algoritmo de Euclides e o Teorema de Bachet-Bézout

1 mdc, mmc e Algoritmo de Euclides

Dados dois números inteiros a e b com $a \neq 0$ ou $b \neq 0$, a cada um deles pode-se associar seu conjunto de divisores positivos, D_a e D_b respectivamente, e a intersecção de tais conjuntos $D_a \cap D_b$ é finita (pela "limitação") e não vazia (já que 1 pertence à intersecção). Por ser finito, $D_a \cap D_b$ possui elemento máximo, que é chamado de *máximo divisor comum* (mdc) dos números a e b. Denotamos este número por $\text{mdc}(a, b)$ (alguns autores usam a notação (a, b)). Para $a = b = 0$ convencionamos $\text{mdc}(0, 0) = 0$. Quando $\text{mdc}(a, b) = 1$ dizemos que a e b são *primos entre si*.

Por outro lado, se denotamos por M_n o conjunto dos múltiplos positivos de n, dados dois números inteiros a e b com $a \neq 0$ e $b \neq 0$, então a intersecção $M_a \cap M_b$ é não vazia (já que $|ab|$ está na intersecção). Como os naturais são bem ordenados, $M_a \cap M_b$ possui elemento mínimo. Tal número é chamado *mínimo múltiplo comum* (mmc) de a e b e o denotaremos por $\text{mmc}(a, b)$ (alguns autores escrevem $[a, b]$).

Para calcularmos o mdc e o mmc de maneira eficiente, vamos descrever o chamado *algoritmo de Euclides* ou *algoritmo das divisões sucessivas*. Primeiramente, vamos relembrar o conceito de *divisão euclidiana*, ou *divisão com resto*, que é uma das quatro operações que toda criança aprende na escola. Sua formulação precisa é: dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem $q, r \in \mathbb{Z}$ com

$$a = bq + r \qquad \text{e} \qquad 0 \leq r < |b|.$$

Tais q e r estão unicamente determinados pelas duas condições acima (veja o argumento a seguir) e são chamados o *quociente* e *resto* da divisão de a por b. O resto r é também denotado por $a \bmod b$.

Para $x \in \mathbb{R}$, definimos o *piso* ou *parte inteira* $\lfloor x \rfloor$ de x como sendo o único $k \in \mathbb{Z}$ tal que $k \leq x < k + 1$; definimos o *teto* $\lceil x \rceil$ de x como o único $k \in \mathbb{Z}$ tal que $k - 1 < x \leq k$. Por exemplo, temos $\lfloor \sqrt{2} \rfloor = 1$, $\lceil \sqrt{2} \rceil = 2$, $\lfloor 10 \rfloor = \lceil 10 \rceil = 10$,

$\lfloor -\pi \rfloor = -4$ e $\lceil -\pi \rceil = -3$. Podemos agora mostrar a existência de q e r satisfazendo as duas condições acima: basta tomar

$$q = \begin{cases} \lfloor a/b \rfloor & \text{se } b > 0 \\ \lceil a/b \rceil & \text{se } b < 0 \end{cases} \qquad \text{e} \qquad r = a - bq \quad \text{em ambos os casos}$$

e é fácil verificar que $0 \leq r < |b|$ a partir das definições das funções piso e teto. Por outro lado, se $a = bq_1 + r_1 = bq_2 + r_2$ com $0 \leq r_1, r_2 < |b|$, então temos que $r_2 - r_1 = b(q_1 - q_2)$ é um múltiplo de b com $|r_2 - r_1| < |b|$, portanto $r_2 - r_1 = 0$ e assim $q_1 = q_2$ também, o que prova a unicidade.

Podemos agora descrever o *algoritmo de Euclides* para calcular o mdc, que se baseia na seguinte simples observação:

Lema 1 (Euclides). *Se $a = bq + r$, então* $\text{mdc}(a, b) = \text{mdc}(b, r)$.

Demonstração. Basta mostrar que $D_a \cap D_b = D_b \cap D_r$, já que se estes conjuntos forem iguais em particular os seus máximos também serão iguais. Se $d \in D_a \cap D_b$ temos $d \mid a$ e $d \mid b$, logo $d \mid a - bq \iff d \mid r$ e portanto $d \in D_b \cap D_r$. Da mesma forma, se $d \in D_b \cap D_r$ temos $d \mid b$ e $d \mid r$, logo $d \mid bq + r \iff d \mid a$ e assim $d \in D_a \cap D_b$. □

O algoritmo de Euclides consiste na aplicação reiterada do lema acima onde q e r são o quociente e o resto na divisão de a por b (note que o lema vale mesmo sem a condição $0 \leq r < |b|$). Como os restos formam uma sequência estritamente decrescente, o algoritmo eventualmente para quando atingimos o resto 0.

Exemplo 2. *Calcule* $\text{mdc}(1001, 109)$.

Solução: Realizando as divisões sucessivas, temos

$$\begin{aligned} 1001 &= 109 \cdot 9 + 20 \\ 109 &= 20 \cdot 5 + 9 \\ 20 &= 9 \cdot 2 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Assim, temos $\text{mdc}(1001, 109) = \text{mdc}(109, 20) = \text{mdc}(20, 9) = \text{mdc}(9, 2) = \text{mdc}(2, 1) = \text{mdc}(1, 0) = 1$. □

Exemplo 3. *Sejam $m \neq n$ dois números naturais. Demonstrar que*

$$\text{mdc}(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & \text{se } a \text{ é par,} \\ 2 & \text{se } a \text{ é ímpar.} \end{cases}$$

Solução: Suponha sem perda de generalidade que $m > n$ e observe a fatoração

$$a^{2^m} - 1 = (a^{2^{m-1}} + 1)(a^{2^{m-2}} + 1)(a^{2^{m-3}} + 1) \ldots (a^{2^n} + 1)(a^{2^n} - 1)$$

Logo $a^{2^m}+1 = (a^{2^n}+1)\cdot q + 2$ com $q \in \mathbb{Z}$ e assim

$$\text{mdc}(a^{2^m}+1, a^{2^n}+1) = \text{mdc}(a^{2^n}+1, 2)$$

que é igual a 2 se $a^{2^n}+1$ for par, isto é, se a for ímpar, e é igual a 1 caso contrário. □

Além de servir de ferramenta computacional para o cálculo do mdc, a divisão euclidiana tem consequências teóricas importantes. O próximo teorema mostra que é sempre possível escrever o mdc de dois números como combinação linear destes (com coeficientes inteiros).

Teorema 4 (Bachet-Bézout). *Sejam $a, b \in \mathbb{Z}$. Então existem $x, y \in \mathbb{Z}$ com*

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

Portanto se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$ então $c \mid \text{mdc}(a, b)$.

Demonstração. O caso $a = b = 0$ é trivial (temos $x = y = 0$). Nos outros casos, considere o conjunto de todas as combinações $\mathbb{Z}$-lineares de a e b:

$$I(a, b) \stackrel{\text{def}}{=} \{ax + by : x, y \in \mathbb{Z}\}$$

Seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a, b)$ (há pelo menos um elemento positivo, verifique!). Afirmamos que d divide todos os elementos de $I(a, b)$. De fato, dado $m = ax + by \in I(a, b)$, sejam $q, r \in \mathbb{Z}$ o quociente e o resto na divisão euclidiana de m por d, de modo que $m = dq + r$ e $0 \leq r < d$. Temos

$$r = m - dq = a(x - qx_0) + b(y - qy_0) \in I(a, b).$$

Mas como $r < d$ e d é o menor elemento positivo de $I(a, b)$, segue que $r = 0$ e portanto $d \mid m$.

Em particular, como $a, b \in I(a, b)$ temos que $d \mid a$ e $d \mid b$, logo $d \leq \text{mdc}(a, b)$. Note ainda que se $c \mid a$ e $c \mid b$, então $c \mid ax_0 + by_0 \iff c \mid d$. Tomando $c = \text{mdc}(a, b)$ temos que $\text{mdc}(a, b) \mid d$ o que, juntamente com a desigualdade $d \leq \text{mdc}(a, b)$, mostra que $d = \text{mdc}(a, b)$. □

Corolário 5. *Sejam $a, b, c \in \mathbb{Z}$. A equação*

$$ax + by = c$$

admite solução inteira em x e y se, e somente se, $\text{mdc}(a, b) \mid c$.

Demonstração. Se a equação admite solução inteira, então $\text{mdc}(a, b)$ divide o lado esquerdo, logo deve dividir o direito também. Reciprocamente, se $\text{mdc}(a, b) \mid c$, digamos $c = k \cdot \text{mdc}(a, b)$ com $k \in \mathbb{Z}$, pelo teorema acima existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = \text{mdc}(a, b)$ e multiplicando tudo por k obtemos que $x = kx_0$ e $y = ky_0$ são soluções da equação dada. □

Temos uma outra importante consequência do teorema anterior:

Proposição 6. *Se* $\text{mdc}(a,b) = 1$ *e* $a \mid bc$*, então* $a \mid c$*.*

Demonstração. Como $\text{mdc}(a,b) = 1$, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1 \implies a \cdot cx + (bc) \cdot y = c$. Do fato de a dividir cada termo do lado esquerdo, temos que $a \mid c$. □

Lembramos que um natural $p > 1$ é chamado *primo* se os únicos divisores positivos de p são 1 e p e um natural $n > 1$ é chamado *composto* se admite outros divisores além de 1 e n. Observemos que 1 não é nem primo nem composto.

Claramente, se p é primo e $p \nmid a$ temos $\text{mdc}(p,a) = 1$. Usando a proposição anterior e indução temos o seguinte resultado:

Corolário 7. *Seja* p *um número primo e sejam* $a_1, \ldots a_m \in \mathbb{Z}$*. Se* $p \mid a_1 \cdots a_m$*, então* $p \mid a_i$ *para algum* i*,* $1 \leq i \leq m$*.*

O próximo lema resume algumas propriedades úteis do mdc:

Lema 8. *Temos*

1. *Se* p *é primo, então* $\text{mdc}(a,p)$ *é* 1 *ou* p*.*
2. *Se* k *é um inteiro, então* $\text{mdc}(a,b) = \text{mdc}(a - kb, b)$*.*
3. *Se* $a \mid c$*, então* $\text{mdc}(a,b) \mid \text{mdc}(c,b)$*.*
4. *Se* $\text{mdc}(a,b) = 1$*, então* $\text{mdc}(ac,b) = \text{mdc}(c,b)$*.*

Demonstração. O primeiro item é claro e o segundo é apenas uma reformulação do lema 1. Para provar o terceiro item, observe que $\text{mdc}(a,b) \mid a$ e $a \mid c$ implicam que $\text{mdc}(a,b) \mid c$. Como também temos $\text{mdc}(a,b) \mid b$, concluímos que $\text{mdc}(a,b) \mid \text{mdc}(b,c)$ por Bachet-Bézout. Finalmente, para mostrar o último item, note primeiro que $\text{mdc}(c,b) \mid \text{mdc}(ac,b)$ pois $\text{mdc}(c,b)$ divide simultaneamente ac e b. Reciprocamente, para mostrar que $\text{mdc}(ac,b) \mid \text{mdc}(c,b)$, podemos escrever $ax + by = 1$ com $x, y \in \mathbb{Z}$ por Bachet-Bézout. Assim, $\text{mdc}(ac,b)$ divide $ac \cdot x + b \cdot cy = c$ e também divide b, logo divide $\text{mdc}(c,b)$. □

Vejamos como podemos usar as propriedades acima para solucionar o seguinte

Exemplo 9. *Sejam* $a_n = 100 + n^2$ *e* $d_n = \text{mdc}(a_n, a_{n+1})$*. Calcular* d_n *para todo* n*.*

Solução: Aplicando a propriedade 2 temos que

$$d_n = \text{mdc}(100 + n^2, 100 + (n+1)^2) = \text{mdc}(100 + n^2, 2n + 1).$$

Como $2n + 1$ é ímpar, $\text{mdc}(4, 2n+1) = 1$ e pelas propriedades 4 e 2 temos que

$$\begin{aligned} d_n &= \text{mdc}(400 + 4n^2, 2n + 1) \\ &= \text{mdc}(400 + 4n^2 - (2n+1)(2n-1), 2n + 1) \\ &= \text{mdc}(401, 2n + 1). \end{aligned}$$

Como 401 é primo, então $\text{mdc}(401, 2n+1) = 401$ se $2n+1 = 401k$ (com $k = 2r+1$ inteiro ímpar) e $\text{mdc}(401, 2n+1) = 1$ caso contrário, ou seja,

$$d_n = \begin{cases} 401 & \text{se } n = 401r + 200 \text{ com } r \in \mathbb{Z} \\ 1 & \text{caso contrário.} \end{cases}$$

□

A próxima proposição conecta o mdc e o mmc de dois inteiros e pode ser utilizada, juntamente com o algoritmo de Euclides, para o cálculo eficiente do mmc.

Proposição 10. *Sejam a e b dois números naturais, então*

$$\text{mdc}(a, b) \cdot \text{mmc}(a, b) = a \cdot b.$$

Demonstração. Escreva $d = \text{mdc}(a, b)$ e $a = a_1 d$ e $b = b_1 d$ onde $a_1, b_1 \in \mathbb{Z}$ são tais que $\text{mdc}(a_1, b_1) = 1$. Temos $\text{mmc}(a, b) = al$ para algum $l \in \mathbb{Z}$; além disso, $b \mid \text{mmc}(a, b) \iff b_1 d \mid a_1 dl \iff b_1 \mid a_1 l$. Como $\text{mdc}(a_1, b_1) = 1$, isto implica que $b_1 \mid l$ pela proposição 6. Pela definição de mínimo múltiplo comum, temos que l deve ser o mínimo número divisível por b_1, assim concluímos que $l = b_1$ e portanto $\text{mmc}(a, b) = b_1 a$. Logo $\text{mdc}(a, b) \cdot \text{mmc}(a, b) = d \cdot b_1 a = a \cdot b$. □

A demonstração que demos do teorema de Bachet-Bézout não mostra como efetivamente encontrar uma solução de $ax + by = \text{mdc}(a, b)$. Porém, isto pode ser feito utilizando-se o algoritmo de Euclides, como mostra o exemplo a seguir. De fato, este exemplo pode servir como ponto de partida para uma segunda demonstração do teorema de Bachet-Bézout (veja os exercícios).

Exemplo 11. *Encontre todos os $x, y \in \mathbb{Z}$ tais que*

$$1001x + 109y = \text{mdc}(1001, 109).$$

Solução: Fazemos as divisões sucessivas para o cálculo de

$$\text{mdc}(1001, 109) = 1$$

utilizando o algoritmo de Euclides (veja o exemplo 2). Em seguida, isolamos os restos:

$$\begin{aligned} \boxed{20} &= \boxed{1001} - \boxed{109} \cdot 9 \\ \boxed{9} &= \boxed{109} - \boxed{20} \cdot 5 \\ \boxed{2} &= \boxed{20} - \boxed{9} \cdot 2 \\ \boxed{1} &= \boxed{9} - \boxed{2} \cdot 4 \end{aligned}$$

Note que a última divisão permite expressar o mdc 1 como combinação linear de 9 e 2:

$$\boxed{9} \cdot 1 - \boxed{2} \cdot 4 = 1.$$

Mas da penúltima divisão, temos que $\boxed{2} = \boxed{20} - \boxed{9} \cdot 2$, logo substituindo esta expressão na combinação linear acima, temos

$$\boxed{9} - (\boxed{20} - \boxed{9} \cdot 2) \cdot 4 = 1 \iff \boxed{9} \cdot 9 - \boxed{20} \cdot 4 = 1$$

e agora expressamos 1 como combinação linear de 20 e 9. Repetindo este procedimento, eventualmente expressaremos 1 como combinação linear de 1001 e 109. Tomamos o cuidado de $\boxed{\text{lembrar}}$ quais são os "coeficientes" a e b nas equações $ax + by = \text{mdc}(a, b)$ durante as simplificações. Continuando, obtemos

$$1 = (\boxed{109} - \boxed{20} \cdot 5) \cdot 9 - \boxed{20} \cdot 4 = \boxed{109} \cdot 9 - \boxed{20} \cdot 49$$
$$1 = \boxed{109} \cdot 9 - (\boxed{1001} - \boxed{109} \cdot 9) \cdot 49 = \boxed{1001} \cdot (-49) + \boxed{109} \cdot 450$$

Logo uma solução da equação $1001x + 109y = 1$ é $(x_0, y_0) = (-49, 450)$. Para encontrar as demais, escrevemos o lado direito desta equação utilizando a solução particular que acabamos de encontrar:

$$1001x + 109y = 1001x_0 + 109y_0 \iff 1001(x - x_0) = -109(y - y_0).$$

Como $\text{mdc}(1001, 109) = 1$ temos pela proposição 6 que 1001 divide $y - y_0$, ou seja, $y - y_0 = 1001t$ para algum $t \in \mathbb{Z}$ e, portanto, $x - x_0 = -109t$. Assim, as soluções da equação dada são todos os pontos da reta $1001x + 109y = 1$ da forma

$$(x, y) = (x_0 - 109t, y_0 + 1001t) = (-49, 450) + (-109, 1001) \cdot t$$

com $t \in \mathbb{Z}$. □

Em geral, o raciocínio do exemplo acima mostra que se $\text{mdc}(a, b) = 1$ e (x_0, y_0) é uma solução da equação $ax + by = c$, então todas as soluções inteiras são dadas por $x = x_0 - bk$ e $y = y_0 + ak$ com $k \in \mathbb{Z}$.

Exemplo 12. *Sejam a, b inteiros positivos com $\text{mdc}(a, b) = 1$. Mostre que para todo $c \in \mathbb{Z}$ com $c > ab - a - b$, a equação $ax + by = c$ admite soluções inteiras com $x, y \geq 0$.*

Solução: Seja (x_0, y_0) uma solução inteira (que existe pelo teorema de Bachet-Bézout). Devemos mostrar a existência de um inteiro k tal que

$$x = x_0 - bk > -1 \qquad \text{e} \qquad y = y_0 + ak > -1,$$

ou seja,

$$-\frac{y_0 + 1}{a} < k < \frac{x_0 + 1}{b}.$$

Mas isto segue do fato de o intervalo $(-\frac{y_0+1}{a}, \frac{x_0+1}{b})$ ter tamanho maior do que 1:

$$\frac{x_0 + 1}{b} - \left(-\frac{y_0 + 1}{a}\right) = \frac{ax_0 + by_0 + a + b}{ab} = \frac{c + a + b}{ab} > 1.$$

□

Problemas Propostos

Problema 13. *Mostre que*

(a) $2^{15} - 1$ *e* $2^{10} + 1$ *são primos entre si.*

(b) $2^{32} + 1$ *e* $2^4 + 1$ *são primos entre si.*

Problema 14 (IMO1992)**.** *Encontrar todos os inteiros* a, b, c *com* $1 < a < b < c$ *tais que* $(a-1)(b-1)(c-1)$ *é divisor de* $abc - 1$*.*

Problema 15. *Mostre que, se* $n > 1$*, então*

$$\sum_{k=1}^{n} \frac{1}{k} = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

não é um número inteiro.

Problema 16 (OBM1997)**.** *Sejam* $c \in \mathbb{Q}$*,* $f(x) = x^2 + c$*. Definimos*

$$f^0(x) = x, \quad f^{n+1}(x) = f(f^n(x)), \forall n \in \mathbb{N}.$$

Dizemos que $x \in \mathbb{R}$ *é pré-periódico se* $\{f^n(x), n \in \mathbb{N}\}$ *é finito. Mostre que* $\{x \in \mathbb{Q} |\, x$ *é pré-periódico*$\}$ *é finito.*

Problema 17. *Demonstrar que se* $\mathrm{mdc}(a, 2^{n+1}) = 2^n$ *e* $\mathrm{mdc}(b, 2^{n+1}) = 2^n$*, então* $\mathrm{mdc}(a + b, 2^{n+1}) = 2^{n+1}$*.*

Problema 18. *Demonstrar que se* a*,* b*,* c*,* d*,* m *e* n *são inteiros tais que* $ad - bc = 1$ *e* $mn \neq 0$*, então*

$$\mathrm{mdc}(am + bn, cm + dn) = \mathrm{mdc}(m, n).$$

Problema 19. *Seja* F_n *o* n*-ésimo termo da sequência de Fibonacci.*

(a) Encontrar dois números inteiros a *e* b *tais que* $233a + 144b = 1$ *(observe que* 233 *e* 144 *são termos consecutivos da sequência de Fibonacci).*

(b) Mostre que $\mathrm{mdc}(F_n, F_{n+1}) = 1$ *para todo* $n \geq 0$*.*

(c) Determine x_n *e* y_n *tais que* $F_n \cdot x_n + F_{n+1} \cdot y_n = 1$*.*

Problema 20. *Sejam* a *e* b *dois inteiros positivos e* d *seu máximo divisor comum. Demonstrar que existem dois inteiros positivos* x *e* y *tais que* $ax - by = d$*.*

Problema 21. *Definimos a* sequência de frações de Farey *de ordem* n *como o conjunto de frações reduzidas* $\frac{a}{b}$ *tais que* $0 \leq \frac{a}{b} \leq 1$*,* $1 \leq b \leq n$*. Por exemplo a sequência de Farey de ordem* 3 *é* $\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$*.*

(a) Demonstrar que se $\frac{a}{b}$ *e* $\frac{c}{d}$ *são dois termos consecutivos de uma sequência de Farey, então* $cb - ad = 1$*.*

(b) Demonstrar que se $\frac{a_1}{b_1}$, $\frac{a_2}{b_2}$, $\frac{a_3}{b_3}$ *são três termos consecutivos de uma sequência de Farey, então* $\frac{a_2}{b_2} = \frac{a_1+a_3}{b_1+b_3}$.

Problema 22. *Utilize indução em* $\min\{a, b\}$ *e o algoritmo de Euclides para mostrar que* $ax + by = \mathrm{mdc}(a, b)$ *admite solução com* $x, y \in \mathbb{Z}$*, obtendo uma nova demonstração do teorema de Bachet-Bézout.*

Problema 23. *Sejam* a *e* b *números inteiros positivos. Considere o conjunto*

$$C = \{ax + by \mid x, y \in \mathbb{N}\}$$

Lembre-se de que já mostramos no exemplo 12 que todo número maior que $ab - a - b$ *pertence a* C.

(a) Demonstre que o número $ab - a - b$ *não pertence a* C.

(b) Achar a quantidade de números inteiros positivos que não pertencem a C.

Problema 24 (IMO1984)**.** *Dados os inteiros positivos* a*,* b *e* c*, dois a dois primos entre si, demonstrar que* $2abc - ab - bc - ca$ *é o maior número inteiro que não pode expressar-se na forma* $xbc + yca + zab$ *com* x*,* y *e* z *inteiros não negativos.*

Problema 25 (IMO1977)**.** *Sejam* a, b *inteiros positivos. Quando dividimos* $a^2 + b^2$ *por* $a + b$*, o quociente é* q *e o resto é* r*. Encontrar todos os* a, b *tais que* $q^2 + r = 1977$.

Problema 26. *Demonstrar que* $\mathrm{mdc}(2^a - 1, 2^b - 1) = 2^{\mathrm{mdc}(a,b)} - 1$ *para todo* $a, b \in \mathbb{N}$.

Problema 27. *Encontrar todas as funções* $f : \mathbb{N}^* \times \mathbb{N}^* \longrightarrow \mathbb{Z}$ *satisfazendo simultaneamente as seguintes propriedades*

(i) $f(a, a) = a$.

(ii) $f(a, b) = f(b, a)$.

(iii) Se $a > b$*, então* $f(a, b) = \frac{a}{a-b} f(a - b, b)$.

Dicas e Soluções

14. Mostrar primeiro que $a \leq 4$ e considerar os possíveis casos.

15. Considere a maior potência de 2 que é menor ou igual a n.

16. Mostre que, dado c racional, existe $M > 0$ tal que, se $|x| > M$, então $|f(x)| > |x|$, e existe um inteiro positivo s tal que, se x é um racional cujo denominador, em sua representação reduzida, é $q > s$, então o denominador de $f(x)$ (em sua representação reduzida) é estritamente maior que q.

18. Observe que $d(am+bn)-b(cm+dn) = m$ e $-c(am+bn)+a(cm+dn) = n$.

21. Vamos provar que os dois itens valem para todo inteiro positivo n, por indução. Isto é facilmente verificável para $n = 1$ e $n = 2$. Considere agora a sequência de frações de Farey de ordem $n + 1$, e seja $\frac{u}{n+1}$ uma fração irredutível em $(0, 1)$. Seus dois vizinhos nessa sequência de Farey têm denominadores menor que $n+1$ (as distâncias de $\frac{u}{n+1}$ às frações mais próximas de denominador n são menores que $\frac{1}{n}$, e são múltiplos inteiros de $\frac{1}{n(n+1)}$, donde são menores ou iguais a $\frac{1}{n+1}$). Sejam $\frac{a}{b}$ e $\frac{c}{d}$ esses dois vizinhos, com $\frac{a}{b} < \frac{u}{n+1} < \frac{c}{d}$. Temos $\frac{u}{n+1} - \frac{a}{b} = \frac{v}{b(n+1)}$ e $\frac{c}{d} - \frac{u}{n+1} = \frac{w}{d(n+1)}$, para certos inteiros positivos v e w, donde $\frac{v}{b(n+1)} + \frac{w}{d(n+1)} = \frac{c}{d} - \frac{a}{b} = \frac{1}{bd}$ (por hipótese de indução, pois $\frac{a}{b}$ e $\frac{c}{d}$ são vizinhos na sequência de Farey de ordem n), ou seja $n+1 = vd+wb \geq b+d$. Como $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$, e $\frac{a}{b}$ e $\frac{c}{d}$ são os vizinhos de $\frac{u}{n+1}$, segue que $\frac{u}{n+1} = \frac{a+c}{b+d}$. Temos $(a+c)b-a(b+d) = cb - ad = 1$ e $c(b + d) - (a + c)d = cb - ad = 1$, e as duas afirmações seguem por indução.

24. Se $2abc - ab - bc - ca = xbc + yca + zab$ com x, y e z inteiros positivos, a divide $(x + 1)bc$, donde $x \geq a - 1$; analogamente, $y \geq b - 1$ e $z \geq c - 1$, donde $xbc + yca + zab \geq 3abc - ab - bc - ca > 2abc - ab - bc - ca$.

    Seja agora $k > 2abc - ab - bc - ca$ inteiro. Então, como $1 = \text{mdc}(bc, a) = \text{mdc}(bc, \text{mdc}(ca, ab))$, k se escreve como $ubc+vca+wab$, para certos u, v, w inteiros. Como $ubc+vca+wab = (u-ta)bc+(v-sb)ca+(w+(t+s)c)ab$, para quaisquer t, s inteiros, podemos supor sem perda de generalidade que $0 \leq u \leq a-1$ e $0 \leq v \leq b-1$. Assim, $ubc+vca \leq (a-1)bc+(b-1)ac = 2abc-bc-ca$, donde $wab = k-(ubc+vca) \geq k-(2abc-bc-ca) > -ab$, e logo $w \geq 0$.

26. Pelo algoritmo de Euclides aplicado aos expoentes, basta mostrar que $\text{mdc}(2^{bq+r} - 1, 2^b - 1) = \text{mdc}(2^b - 1, 2^r - 1)$. Mas isto segue novamente do lema de Euclides, pois $2^{bq+r} - 1 = 2^r(2^{bq} - 1) + 2^r - 1$ e $2^{bq} - 1 = (2^b - 1)(2^{b(q-1)} + 2^{b(q-2)} + \cdots + 2^b + 1)$ é um múltiplo de $2^b - 1$.

27. Prove por indução em $a + b$ que $f(a, b) = \text{mmc}(a, b)$ para quaisquer $a, b \in \mathbb{N}^*$.

Referências

[1] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.