Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 2

Prof. Samuel Feitosa

Aula 3

O Algoritmo de Euclides

Exemplo 1. *Seja S um conjunto infinito de inteiros não negativos com a seguinte propriedade: dados dois quaisquer de seus elementos, o valor absoluto da diferença entre eles também pertence a S. Se d é o menor elemento positivo de S, prove que S consiste de todos os múltiplos de d.*

Considere um elemento m qualquer de S. Pelo algoritmo da divisão, $m = qd + r$ com $0 \leq r < d$. Como todos os números $m - d, m - 2d, m - 3d, \ldots, m - qd = r$ pertencem a S e d é o menor elemento positivo de tal conjunto, devemos ter obrigatoriamente que $r = 0$. Sendo assim, podemos concluir que todos os elementos de S são múltiplos de d. Resta mostrarmos que todos os múltiplos de d estão em S. Seja kd um múltiplo positivo qualquer de d. Como S é infinito, existe um inteiro $m \in S$ tal que $m = qd > kd$. Assim todos os números $m - d, m - 2d, \ldots, m - (q - k)d = kd$ estão em S.

Definição 2. *Um inteiro a é um divisor comum de b e c se $a \mid b$ e $a \mid c$. Se b e c não são ambos nulos, denotaremos por $mdc(b, c)$ o máximo divisor comum de b e c.*

Como um inteiro não nulo possui apenas um número finito de divisores, se b e c são ambos não nulos, o número $mdc(b, c)$ sempre existe, isto é, sempre está bem definido.

Lema 3. *(Euclides) Se $x \neq 0$, $mdc(x, y) = mdc(x, x + y)$*

Demonstração. Seja d um divisor comum de x e y. Então $d \mid x + y$ e consequentemente d também á um divisor comum de x e $x + y$. Reciprocamente, se f é um divisor comum de $x + y$ e x, f também divide $(x + y) - y = x$ e assim f é um divisor comum de x e y. Como os conjuntos de divisores comuns dos dois pares de números mencionados são os mesmos, o maior divisor comum também é o mesmo. □

Então podemos calcular:

$$mdc(123, 164) = mdc(123, 41) = mdc(41, 123) = mdc(41, 82) = mdc(41, 41) = 41.$$

Exemplo 4. *Três máquinas I, R, S imprimem pares de inteiros positivos em tickets. Para a entrada (x, y), as máquinas I, R, S imprimem respectivamente $(x-y, y), (x+y, y), (y, x)$. Iniciando com o par $(1, 2)$ podemos alcançar*

a) (819, 357)?

b) (19, 79)?

Para o item a), calculemos inicialmente $mdc(819, 357)$:

$mdc(819, 357) = mdc(462, 357) = mdc(105, 357) = mdc(105, 252) = \ldots = mdc(21, 21) = 21.$

Pelo Lema de Euclides, o mdc entre os dois números em um ticket nunca muda. Como $mdc(1, 2) = 1 \neq 21 = mdc(819, 357)$, não podemos alcançar o par do item a).

Para o item b), indiquemos com $\rightarrow$ uma operação de alguma das máquinas. Veja que: $(2, 1) \stackrel{R}{\rightarrow} (3, 1) \stackrel{S}{\rightarrow} (1, 3) \stackrel{R}{\rightarrow} (4, 3) \stackrel{R}{\rightarrow} \ldots \stackrel{R}{\rightarrow} (19, 3) \stackrel{S}{\rightarrow} (3, 19) \stackrel{R}{\rightarrow} (22, 19) \stackrel{R}{\rightarrow} (41, 19) \stackrel{R}{\rightarrow} (60, 19) \stackrel{R}{\rightarrow} (79, 19)$.

Observação 5. *Procurar* **invariantes** *sempre é uma boa estratégia para comparar configurações diferentes envolvidas no problema. Confira o problema proposto 31.*

Definição 6. *Dizemos que dois inteiros p e q são primos entre si ou relativamente primos se $mdc(p, q) = 1$. Dizemos ainda que a fração $\frac{p}{q}$ é irredutível se p e q são relativamente primos.*

Exemplo 7. *(IMO 1959) Prove que $\dfrac{21n+4}{14n+3}$ é irredutível para todo número natural n.*

Pelo lema de Euclides, $mdc(21n+4, 14n+3) = mdc(7n+4, 14n+3) = mdc(7n+1, 7n+2) = mdc(7n+1, 1) = 1$.

O seguinte lema será provado na próxima aula.

Lema 8. *(Propriedades do MDC) Seja $mdc(a, b) = d$, então:*

i) Se $k \neq 0$, $mdc(ka, kb) = kd$.

ii) $mdc\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.

iii) Se $mdc(a, c) = 1$, então $mdc(a, bc) = d$.

Exemplo 9. *(Olimpíada Inglesa) Se x e y são inteiros tais que $2xy$ divide x^2+y^2-x, prove que x é um quadrado perfeito*

Se $d = mdc(x, y)$, então $x = da$ e $y = db$, com $mdc(a, b) = 1$. Do enunciado, temos:

$$\begin{aligned} 2abd^2 \mid d^2a^2 + d^2b^2 - da &\Rightarrow \\ d^2 \mid d^2a^2 + d^2b^2 - da &\Rightarrow \\ d^2 \mid -da &\Rightarrow \\ d \mid a. & \end{aligned}$$

Logo, $a = dc$, para algum c. Como $x \mid y^2$, obtemos $d^2c \mid d^2b^2$, ou seja, $c|b^2$ e $mdc(c, b^2) = c$. Usando que $mdc(a, b) = 1$ e que todo divisor comum de b e c também é um divisor comum de a e b, podemos concluir que $mdc(c, b) = 1$. Usando o item *iii)* do lema anterior, $mdc(c, b^2) = 1$. Assim, $c = 1$ e $x = d^2c = d^2$.

Exemplo 10. *No planeta X, existem apenas dois tipos de notas de dinheiro: \$5 e \$78. É possível pagarmos exatamente \$7 por alguma mercadoria? E se as notas fossem de \$ 3 e \$ 78?*

Veja que $2 \times 78 - 31 \times 5 = 1$ e consequentemente $14 \times 78 - 217 \times 5 = 7$. Basta darmos 14 notas de de \$ 78 para recebermos 217 notas de \$ 5 como troco na compra de nossa mercadoria. Usando as notas de \$3 e \$78 não é possível pois o dinheiro pago e recebido como troco por algo sempre é múltiplo de 3 e 7 não é múltiplo de 3.

Queremos estudar a versão mais geral desse exemplo. Quais são os valores que podemos pagar usando notas de $\$a$ e $\$b$? Em particular, estaremos interessados em conhecer qual o menor valor que pode ser pago. Para responder essa pergunta, precisaremos do algoritmo de Euclides:

Teorema 11. *(O Algoritmo de Euclides) Para os inteiros b e $c > 0$, aplique sucessivamente o algoritmo da divisão para obter a série de equações:*

$$\begin{aligned} b &= cq_1 + r_1, \ 0 < r_1 < c, \\ c &= r_1q_2 + r_2, \ 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, \ 0 < r_3 < r_2, \\ &\vdots \\ r_{j-2} &= r_{j-1}q_j + r_j, \ 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_jq_{j+1} \end{aligned}$$

A sequência de restos não pode diminuir indefinidamente pois $0 \leq r_i < r_{i-1}$ e existe apenas um número finito de naturais menores que c. Assim, para algum j, obteremos $r_{j+1} = 0$. O maior divisor comum de b e c será r_j, ou seja, o último resto não nulo da sequência de divisões acima.

Demonstração. Pelo Lema de Euclides,

$$mdc(x + qy, y) = mdc(x + (q - 1)y, y) = mdc(x + (q - 2)y, y) = \ldots = mdc(x, y).$$

Então,

$$mdc(b,c) = mdc(c,r_1) = mdc(r_1,r_2) = \ldots = mdc(r_{j-1},r_j) = r_j.$$

□

Exemplo 12. *Calcule* $mdc(42823, 6409)$.

Pelo Algoritmo de Euclides,

$$\begin{aligned} 42823 &= 6 \times 6409 + 4369 \\ 6409 &= 1 \times 4369 + 2040 \\ 4369 &= 2 \times 2040 + 289 \\ 2040 &= 7 \times 289 + 17 \\ 289 &= 17 \times 17. \end{aligned}$$

Portanto, $mdc(42823, 6409) = 17$.

Podemos extrair mais informações do Algoritmo de Euclides. Para isso, iremos organizar as equações do exemplo acima de outra forma.

Essencialmente, a equação $mdc(x+qy, y) = mdc(x, y)$ nos diz que podemos subtrair q vezes um número de outro sem alterar o máximo divisor comum do par em questão. Realizando esse procedimento sucessivas vezes, subtraindo o número menor do maior, podemos obter pares com números cada vez menores até que chegarmos em um par do tipo (d, d). Como o máximo divisor comum foi preservado ao longo dessas operações, d será o máximo divisor comum procurado. Iremos repetir o exemplo anterior registrando em cada operação quantas vezes um número é subtraido do outro. Isso será feito através de dois pares de números auxiliares:

$$\begin{aligned} (42823, 6409) &\mid (1,0)(0,1) \\ (4369, 6409) &\mid (1,-6)(0,1) \\ (4369, 2040) &\mid (1,-6)(-1,7) \\ (289, 2040) &\mid (3,-20)(-1,7) \\ (289, 17) &\mid (3,-20)(-22,147) \\ (17, 17) &\mid (355,-2372)(-22,147) \end{aligned}$$

Da primeira linha para a segunda, como subtraímos 6 vezes o número 6409 de 42823, subtraímos 6 vezes o par $(0, 1)$ de $(1, 0)$, obtendo: $(1, 0) - 6(0, 1) = (1, -6)$. Se em uma dada linha, temos:

$$(x, x + qy)) \mid (a, b)(c, d);$$

então, a próxima linha deverá ser:

$$(x, y) \mid (a, b)(c - aq, d - bq);$$

porque representará a operação de subtrairmos q vezes o primeiro número do segundo. Veja que o par (a, b) foi subtraido de (c, d) exatamente q vezes. Os números escritos nos últimos dois pares representam os coeficientes dos números originais para cada número do primeiro par. Por exemplo, analisando a linha:

$$(289, 2040) \mid (3, -20)(-1, 7);$$

obtemos que:

$$\begin{aligned} 289 &= 3 \times 42823 - 20 \times 6409, \\ 2040 &= -1 \times 42823 + 7 \times 6409. \end{aligned}$$

Em cada linha, essa propriedade é mantida pois a mesma subtração que é realizada no primeiro par também é realizada entre os dois últimos pares. Analisando o último par, podemos escrever 17 como combinação de 42823 e 6409 de duas formas diferentes:

$$\begin{aligned} 17 &= -22 \times 42823 + 147 \times 6409, \\ 17 &= 355 \times 42823 + -2372 \times 6409, \end{aligned}$$

Assim, se no planeta X tivéssemos apenas notas de \$42823 e \$6409, poderíamos comprar algo que custasse exatamente \$17.

Como conclusão da discussão anterior e do algoritmo de Euclides, podemos concluir que:

Teorema 13. *(Bachet-Bèzout) Se $d = mdc(a, b)$, então existem inteiros x e y tais que $ax + by = d$.*

De fato, a discussão anterior também nos mostra um algoritmo para encontrarmos x e y. Voltando à discussão sobre o planeta X, podemos concluir em virtude do teorema anterior que qualquer valor múltiplo de d poderá ser pago usando apenas as notas de \$$a$ e \$$b$. Como todo valor pago, necessariamente é um múltiplo do máximo divisor comum de a e b, descobrimos que o conjunto que procurávamos consiste precisamente do conjunto dos múltiplos de d.

Observação 14. *(Para professores) A prova mais comum apresentada para o teorema anterior baseia-se na análise do conjunto de todas as combinações lineares entre a e b e quase sempre se preocupa apenas com mostrar a existência de x e y. Acreditamos que o algoritmo para encontrar x e y facilite o entendimento do teorema para os alunos mais jovens. Entretanto, frequentemente utilizemos apenas a parte da existência descrita no enunciado. Além disso, preferimos discutir um exemplo numérico ao invés de formalizarmos uma prova e sugerimos que o professor faça o mesmo com mais exemplos em aula.*

Exemplo 15. *(Olimíada Russa 1995) A sequência $a_1, a_2, ...$ de naturais satisfaz $mdc(a_i, a_j) = mdc(i, j)$ para todo $i \neq j$ Prove que $a_i = i$ para todo i.*

Para qualquer inteiro n, $mdc(a_{2n}, a_n) = mdc(2n, n) = n$, consequentemente $n \mid a_n$. Seja d um divisor qualquer de a_n diferente de n, então $d \mid mdc(a_d, a_n)$. De $mdc(a_d, a_n) = mdc(d, n)$, podemos concluir que $d \mid n$. Sendo assim, todos os divisores de a_n que são diferentes de n são divisores de n. Como já sabemos que $a_n = nk$, para algum k, não podemos ter $k > 1$ pois nk não divide n e assim concluímos que $a_n = n$.

Exemplo 16. *Mostre que* $mdc(2^{120} - 1, 2^{100} - 1) = 2^{20} - 1$.

Pelo lema de Euclides,

$$\begin{aligned} mdc(2^{120} - 1, 2^{100} - 1) &= mdc(2^{120} - 1 - 2^{20}(2^{100} - 1), 2^{100} - 1), \\ &= mdc(2^{20} - 1, 2^{100} - 1), \\ &= mdc(2^{20} - 1, 2^{100} - 1 - 2^{80}(2^{20} - 1)), \\ &= mdc(2^{20} - 1, 2^{80} - 1), \\ &= mdc(2^{20} - 1, 2^{80} - 1 - 2^{60}(2^{20} - 1)), \\ &= mdc(2^{20} - 1, 2^{60} - 1), \\ &= mdc(2^{20} - 1, 2^{60} - 1 - 2^{40}(2^{20} - 1)), \\ &= mdc(2^{20} - 1, 2^{40} - 1), \\ &= mdc(2^{20} - 1, 2^{40} - 1 - 2^{20}(2^{20} - 1)), \\ &= mdc(2^{20} - 1, 2^{20} - 1) = 2^{20} - 1. \end{aligned}$$

Exemplo 17. *(Olimpíada Russa 1964) Sejam x, y inteiros para os quais a fração*

$$a = \frac{x^2 + y^2}{xy}$$

é inteira. Ache todos os possíveis valores de a.

A primeira estratégia é cancelar os fatores comuns com o objetivo de reduzir o problema ao caso em que x e y são primos entre si. Seja $d = \text{mdc}(x, y)$, com

$$\begin{cases} x &= d \cdot x_0 \\ y &= d \cdot y_0 \end{cases}, \ \text{mdc}(x_0, y_0) = 1,$$

então

$$a = \frac{x^2 + y^2}{xy} = \frac{{x_0}^2 + {y_0}^2}{x_0 y_0}.$$

Nessa condição, como x_0 divide y_0^2 e y_0 divide x_0^2, cada um deles é igual a 1, donde

$$a = \frac{1^2 + 1^2}{1 \cdot 1} = 2.$$

Definição 18. *Os inteiros $a_1, a_2, \ldots, a_n$, todos diferentes de zero, possuem múltiplo comum b se $a_i|b$ para $i = 1, 2, \ldots, n$(note que $a_1a_2 \ldots a_n$ é um múltiplo comum). O menor múltiplo comum positivo para tal conjunto de inteiros é chamado de mínimo múltiplo comum e será denotado por $mmc(a_1, a_2, \ldots, a_n)$.*

Proposição 19. *Se a e b são não nulos, então: $mmc(a, b) \cdot mdc(a, b) = |ab|$.*

(A prova desta proposição também será deixada para a próxima seção)

Exemplo 20. *(Olimpíada Russa 1995) Sejam m e n interios positivos tais que:*

$$mmc(m, n) + mdc(m, n) = m + n.$$

Prove que um deles é divisível pelo o outro.

Se $d = mdc(m, n)$, então podemos escrever $m = da$ e $n = db$. Pela proposição anterior,

$$mmc(m, n) = \frac{d^2ab}{d} = dab.$$

Temos:

$$\begin{aligned} mmc(m, n) + mdc(m, n) - m - n &= 0 \Rightarrow \\ dab + d - da - db &= 0 \Rightarrow \\ ab + 1 - a - b &= 0 \Rightarrow \\ (a - 1)(b - 1) &= 0. \end{aligned}$$

Portanto, ou $a = 1$ e $m \mid n$ ou então $b = 1$ e $n \mid m$.

Exemplo 21. *(Torneio das Cidades 1998) Prove que, para quaisquer inteiros positivos a e b, a equação $mmc(a, a + 5) = mmc(b, b + 5)$ implica que $a = b$.*

Para o item a), como $(a + 5) - a = 5$, temos $mdc(a, a + 5)$ é igual a 1 ou 5. O mesmo vale para $mdc(b, b + 5)$. Pela proposição anterior, temos:

$$\begin{aligned} mmc(a, a + 5) &= \frac{a(a + 5)}{mdc(a, a + 5)}, \\ mmc(b, b + 5) &= \frac{b(b + 5)}{mdc(b, b + 5)}. \end{aligned}$$

Suponha que $mdc(a, a+5) = 5$ e $mdc(b, b+5) = 1$, então $a(a+5) = 5b(b+5)$. Consequentemente, a é múltiplo de 5 e $a(a + 5)$ é múltiplo de 25. Isso implica que $b(b + 5)$ também é múltiplo de 5 e que $mdc(b, b + 5) > 1$. Uma contradição. Analogamente, não podemos ter $mdc(a, a + 5) = 1$ e $mdc(b, b + 5) = 5$. Sendo assim, $mdc(a, a + 5) = mdc(b, b + 5)$ e:

$$\begin{aligned} a(a + 5) - b(b + 5) &= 0 \Rightarrow \\ (a - b)(a + b + 5) &= 0. \end{aligned}$$

Como $a + b + 5 > 0$, concluímos que $a = b$.

Exemplo 22. *Uma máquina f executa operações sobre o conjunto de todos os pares de inteiros positivos. Para cada par de inteiros positivos, ela fornece um inteiro dado pelas regras:*

$$f(x,x) = x,\ f(x,y) = f(y,x),\ (x+y)f(x,y) = yf(x,x+y).$$

Determine $f(2012, 2012! + 1)$.

Claramente $mmc(x,x) = x$ e $mmc(x,y) = mmc(y,x)$. Usando a proposição anterior e o lema de Euclides temos:

$$(x+y)mmc(x,y) = (x+y)\frac{xy}{mdc(x,y)} = y \cdot \frac{x(x+y)}{mdc(x,x+y)} = y \cdot mmc(x,x+y)$$

Temos então uma forte suspeita de que $f = mmc$. Seja S o conjunto de todos os pares de inteiros positivos (x,y) tais que $f(x,y) \neq mmc(x,y)$, e seja (m,n) o par em S com a soma $m+n$ minima. Note que todo par da forma (n,n) não está em S pois $f(n,n) = n = mmc(n,n)$. Assim, devemos ter $m \neq n$. Suponha sem perda de generalidade que $n > m$. Portanto:

$$\begin{aligned} nf(m,n-m) &= [m+(n-m)]f(m,n-m) \Rightarrow \\ &= (n-m)f(m,m+(n-m)) \Rightarrow \\ f(m,n-m) &= \frac{n-m}{n} \cdot f(m,n) \end{aligned}$$

Como o par $(m, m-n)$ não está em S, dado que a soma de seus elementos é menor que $m+n$, temos:

$$\begin{aligned} f(m,n-m) &= mmc(m,n-m) \qquad\qquad \Rightarrow \\ \frac{n-m}{n} \cdot f(m,n) &= (n-m)mmc(m,m+(n-m)) \Rightarrow \\ f(m,n) &= mmc(m,n) \end{aligned}$$

Uma contradição. Desse modo, S deve ser um conjunto vazio e $f(x,y) = mmc(x,y)$ para todos os pares de inteiros positivos. Como $2012 \mid 2012!$, $mdc(2012, 2012! + 1) = 1$ e consequentemente $mmc(2012, 2012! + 1) = 2012(2012! + 1)$.

Problemas Propostos

Problema 23. *Calcule:*

a) $mdc(n, n^2 + n + 1)$.

b) $mdc(3 \times 2012, 2 \times 2012 + 1)$.

c) $mdc\left(\frac{2^{40}+1}{2^8+1}, 2^8+1\right)$.

Problema 24. *Encontre* $mdc(2n+13, n+7)$

Problema 25. *Prove que a fração* $\frac{12n+1}{30n+2}$ *é irredutível.*

Problema 26. *Sejam* a, b, c, d *inteiros não nulos tais que* $ad-bc=1$. *Prove que* $\frac{a+b}{c+d}$ *é uma fração irredutível.*

Problema 27. *Mostre que* $mdc(a^m-1, a^n-1) = a^{mdc(m,n)}-1$.

Problema 28. *Mostre que se* $mdc(a,b)=1$, *então:*

$$mdc(a+b, a^2-ab+b^2) = 1 \text{ ou } 3$$

Problema 29. *Dado que* $mdc(a,4)=2$, $mdc(b,4)=2$, *prove que:*

$$mdc(a+b,4) = 4.$$

Problema 30. *Prove que, para todo natural* n,

$$mdc(n!+1, (n+1)!+1) = 1.$$

Problema 31. *No exemplo 4, determine todos os pares que podem ser obtidos começando-se com o par* $(1,2)$.

Problema 32. *Qual o máximo divisor comum do conjunto de números:*

$$\{16^n + 10n - 1, n = 1, 2, 3 \ldots\}?$$

Problema 33. *A sequência* F_n *de Farey é a sequência de todos as frações irredutíveis* $\frac{a}{b}$ *com* $0 \leq a \leq b \leq n$ *arranjados em ordem crescente.*

$$\begin{aligned}
F_1 &= \{0/1, 1/1\} \\
F_2 &= \{0/1, 1/2, 1/1\} \\
F_3 &= \{0/1, 1/3, 1/2, 2/3, 1/1\} \\
F_4 &= \{0/1, 1/4, 1/3, 1/2, 2/3, 3/4, 1/1\} \\
F_5 &= \{0/1, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 1/1\} \\
F_6 &= \{0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 1/1\}
\end{aligned}$$

Claramente, toda fração $\frac{a}{b} < 1$ *com* $mdc(a,b)=1$, *está em algum* F_n. *Mostre que se* m/n *e* m'/n' *são frações consecutivas em* F_n *temos* $|mn'-nm'|=1$.

Problema 34. *(Resvista Quantum - Jornal Kvant) Todas as frações irredutíveis cujos denominadores não excedem 99 são escritas em ordem crescente da esquerda para a direita:*

$$\frac{1}{99}, \frac{1}{98}, \ldots, \frac{a}{b}, \frac{5}{8}, \frac{c}{d}, \ldots$$

Quais são as frações $\frac{a}{b}$ *e* $\frac{c}{d}$ *em cada lado de* $\frac{5}{8}$*?*

Problema 35. *(OBM) Para cada inteiro positivo $n > 1$, prove que $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ não é inteiro.*

Problema 36. *Determine todas as soluções em inteiros positivos para $\frac{1}{a} + \frac{1}{b} = \frac{1}{c}$.*

Problema 37. *Inteiros positivos a e b, relativamente primos, são escolhidos de modo que $\dfrac{a+b}{a-b}$ seja também um inteiro positivo. Prove que pelo menos um dos números $ab+1$ e $4ab+1$ é um quadrado perfeito.*

Problema 38. *(IMO 1979) Sejam p, q números naturais primos entre si tais que:*

$$\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \ldots - \frac{1}{1318} + \frac{1}{1319}.$$

Prove que p é divisível por 1979.

Respostas, Dicas e Soluções

23. (a)

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

(b)

$$\begin{aligned} mdc(3\times 2012, 2\times 2012+1) &= mdc(3\times 2012-(2\times 2012+1), 2\times 2012+1), \\ &= mdc(2012-1, 2\times 2012+1), \\ &= mdc(2012-1, 2\times 2012+1-2(2012-1)), \\ &= mdc(2012-1, 3), \\ &= mdc(2012-1-3\times 670, 3), \\ &= mdc(2,3) = 1. \end{aligned}$$

Outra opção seria observar que o mdc procurado deve dividir o número $3(2\times 2012+1) - 2(3\times 2012) = 3$ e que $2\times 2012+1$ não é múltiplo de 3.

(c)

$$\begin{aligned} mdc\left(\frac{2^{40}+1}{2^8+1}, 2^8+1\right) &= mdc\left(2^{32}+2^{24}+2^{16}+2^8+1, 2^8+1\right), \\ &= mdc\left((2^{32}-1)+(2^{24}+1)+(2^{16}-1)+(2^8+1)+1, 2^8+1\right), \\ &= mdc(1, 2^8+1) = 1. \end{aligned}$$

24.

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

25.

$$\begin{aligned} mdc(12n+1, 30n+2) &= mdc(12n+1, 30n+2-2(12n+1)), \\ &= mdc(12n+1, 6n), \\ &= mdc(12n+1-2(6n), 6n), \\ &= mdc(1, 6n) = 1 \end{aligned}$$

26. Seja $f = mdc(a+b, c+d)$. Então $f \mid d(a+b) - b(c+d) = 1$ e consequentemente $f = 1$.

27. Veja que

$$\begin{aligned} mdc(a^m - 1, a^n - 1) &= mdc(a^{m-n} - 1 + (a^n - 1)a^{m-n}, a^n - 1) \\ &= mdc(a^{m-n} - 1, a^n - 1) \end{aligned}$$

O resultado segue aplicando o Algoritmo de Euclides aos expoentes.

28. Seja $f = mdc(a+b, a^2 - ab + b^2)$. Então $f \mid (a+b)^2 - (a^2 - ab + b^2) = 3ab$. Se $mdc(f, a) > 0$, devemos ter $mdc(f, b) > 0$ pois $f \mid a + b$. O mesmo argumento vale para $mdc(f, b) > 0$. Assim, $mdc(f, a) = mdc(f, b) = 1$. Portanto, $f \mid 3$.

30. Pelo lema de Euclides,

$$\begin{aligned} mdc(n! + 1, (n+1)! + 1) &= mdc(n! + 1, (n+1)! + 1 - (n+1)(n! + 1)) \\ &= mdc(n! + 1, -n) \\ &= mdc(n! + 1 - n[(n-1)!], -n) = 1 \end{aligned}$$

34. Sejam $l = mmc\{1, 2, \ldots, n\}$ e $a_i = l/i$. A soma considerada é

$$\frac{a_1 + a_2 + \ldots + a_n}{l}.$$

Queremos analisar o expoente do fator 2 no numerador e no denominador. Seja k tal que $2^k \leq n < 2^{k+1}$. Então $2^k || l$ e a_i é par para todo $i \neq 2^k$. Como a_{2^k} é ímpar, segue que o numerador é ímpar enquanto que o denominador é par. Consequentemente a fração anterior não representa um inteiro.

36. Sejam $d = mdc(a, b)$, $a = dx$, $b = dy$. Consequentemente $mdc(x, y) = 1$ e podemos escrever a equação como:

$$\begin{aligned} \frac{1}{a} + \frac{1}{b} &= \frac{1}{c} \Rightarrow \\ bc + ac &= ab \\ dyc + dxc &= d^2xy \\ c(x + y) &= dxy \end{aligned}$$

Como $mdc(xy, x + y) = 1$ pois $mdc(x, y) = 1$, devemos ter $xy \mid c$ e consequentemente $c = xyk$. Assim, $d = k(x + y)$. O conjunto solução é formado pelas triplas (a, b, c) onde $(a, b, c) = (kx(x + y), ky(x + y), xyk)$ com $mdc(x, y) = 1$ e x, y e k inteiros positivos.

38. Use a identidade de Catalão:

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots - \frac{1}{2n} = \frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n}$$

Em seguida, agrupe os termos da forma $\frac{1}{n+i} + \frac{1}{2n-i+1}$ e analise o numerador da fração obtida.

Referências

[1] S. B. Feitosa, B. Holanda, Y. Lima and C. T. Magalhães, Treinamento Cone Sul 2008. Fortaleza, Ed. Realce, 2010.

[2] D. Fomin, A. Kirichenko, Leningrad Mathematical Olympiads 1987-1991, MathPro Press, Westford, MA, 1994.

[3] D. Fomin, S. Genkin and I. Itenberg, Mathematical Circles, Mathematical Words, Vol. 7, American Mathematical Society, Boston, MA, 1966.

[4] I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction to the Theory of Numbers.