Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 2

Prof. Samuel Feitosa

Aula 17

# Aula de Revisão e Aprofundamento

**Exemplo 1.** *O mínimo multiplo comum dos inteiros $a, b, c, d$ e $d$ é igual à $a + b + c + d$. Prove que $abcd$ é divisível por 3 ou por 5.*

**Solução:** Suponha inicialmente que $mdc(a, b, c, d) = 1$ e seja $L = a + b + c + d$. Como $L$ é o mínimo múltiplo comum, existem $x, y, z, w$ tais que $aw = bx = cy = dz = L$. É fácil ver que $L$ também é o mínimo múltiplo comum de $x, y, z, w$ e que

$$\begin{aligned} \frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{w} &= \frac{a}{L} + \frac{b}{L} + \frac{c}{L} + \frac{d}{L} \\ &= 1. \end{aligned}$$

Suponha sem perda de generalidade que $w \leq x \leq y \leq z$. Da equação anterior, o maior valor de $w$ é 4 e ocorrendo igualdade deveríamos ter $a = b = c = d = 1$ que não satisfaz o enunciado. Para $w = 3$, o leitor poderá facilmente verificar que $a = b = 4, c = 3$ e $d = 1$ é a única solução. Para $w = 2$, temos as seguintes soluções: $(a, b, c, d) = (5, 2, 2, 1), (10, 5, 4, 1), (6, 4, 1, 1)$ , $(9, 6, 2, 1), (12, 8, 3, 1), (21, 14, 6, 1)$. Em todos os casos, $L$ é divisível por 3 ou 5.

**Exemplo 2.** *Seja $A = \{a_1 < a_2 < a_3 < \cdots\}$ uma seqüência crescente de inteiros positivos em que o número de fatores primos de cada termo, contando fatores repetidos, nunca é maior que 2007. Prove que é sempre possível extrair do conjunto $A$ um subconjunto infinito*

$$B = \{b_1 < b_2 < b_3 < \cdots\}$$

*tal que o máximo divisor comum entre $b_i$ e $b_j$ é sempre o mesmo para quaisquer naturais $i \neq j$.*

O número de primos usados como fatores dos $a_i$ não pode ser finito, pois se essa quantidade é $n$, teríamos apenas $n^{2007}$ possíveis elementos $a_i$. Podem ocorrer duas situações:

**a) Nenhum primo divide infinitos $a_i$.** Seja $b_1 = a_1$. Como cada fator primo de $a_1$ aparece um número finito de vezes como fator dos $a_i$, existirá um termo $a_l > a_1$ tal que $a_1$ e $a_l$ são primos entre si. Seja $b_2 = a_l$. Esse argumento pode ser repetido para gerar um subconjunto infinito $B = \{b_1 < b_2 < b_3 < \cdots\}$ de modo que $\text{mdc}(b_i, b_j) = 1$, quaisquer que

sejam os naturais $i, j$.

**b) Existe um primo $p$ que divide infinitos $a_i$.** Como o expoente de $p_1 = p$ em cada $a_i$ que é múltiplo de $p_1$ é um elemento do conjunto $\{1, \ldots, 2007\}$, pelo menos um deles, digamos $r_1 > 0$, deverá ocorrer infinitas vezes. Seja $A_1$ o conjunto de todos os termos $a_i$ para os quais o expoente de $p_1$ em $a_i$ é $r_1$. Se nenhum primo $p_2 \neq p_1$ divide infinitos elementos de $A_1$, o caso anterior mostra que $A_1$ possui um subconjunto tal que o máximo divisor comum de quaisquer dois elementos é ${p_1}^{r_1}$. Senão, seja $p_2 \neq p_1$ um primo que divide infinitos elementos de $A_1$. O expoente de $p_2$ em cada elemento de $A_1$ que é múltiplo de $p_2$ pertence ao conjunto $\{1, \ldots, 2007 - r_1\}$. Sejam $r_2 > 0$ um expoente que ocorre infinitas vezes e $A_2$ o conjunto dos elementos de $A_1$ para os quais $p_1$ e $p_2$ têm expoentes $r_1$ e $r_2$, respectivamente. Esse processo deve terminar em $i$ passos, $i \leq 2007$, e nessa situação $A_i$ é um subconjunto de $A$ para o qual todo elemento é um múltiplo de $P = p_1^{r_1} p_2^{r_2} \cdots p_i^{r_i}$, digamos

$$A_i = \{Pc_1 < Pc_2 < Pc_3 < \cdots\},$$

onde C=$\{c_1 < c_2 < c_3 < \cdots\}$ é um conjunto em que cada termo é o produto de não mais que $2007 - (r_1 + r_2 + \cdots + r_i)$ fatores primos, nenhum dos quais ocorrendo infinitas vezes. Pelo caso a), $C$ possui um subconjunto $B_1$ tal que quaisquer dois elementos são primos entre si. O conjunto

$$B = P \cdot B_1 = \{Px \,|\, x \in B_1\}$$

satisfaz as condições do problema, pois o máximo divisor comum entre quaisquer dois de seus elementos é igual a $P$.

**Exemplo 3.** *(Seletiva Rioplatense 2001) Encontre todos os pares $(m, n)$ de números naturais com $m < n$ tais que $m^2 + 1$ é um múltiplo de $n$ e $n^2 + 1$ é um múltiplo de $m$.*

Afirmamos que todas as soluções são da forma $(F_{2k-1}, F_{2k+1}), k \geq 0$ ($F_n$ é o $n$-ésimo termo da sequência de Fibonacci). É fácil ver que $F_{2k-1}F_{2k+3} = F_{2k+1}^2 + 1$ e portanto os pares anteriores são soluções. Seja $P$ o conjunto das soluções que não são da forma $(F_{2k-1}, F_{2k+1})$. O conjunto $P$ contém um par $(a, b)$ tal que $a + b$ é mínimo. Suponhamos $a < b$(se $a = b \Rightarrow (a, b) = (1, 1) = (F_{-1}, F_1) \notin P$). Como $b \mid a^2 + 1$, $a^2 + 1 = bb'$ e $b' < a$. É fácil ver que $a \mid {b'}^2 + 1$ e $b' \mid a^2 + 1$. Logo $(b', a)$ é uma solução com $b' + a < a + b$ Entretanto, $(b', a) \notin P$ e daí $(b', a) = (F_{2k-1}, F_{2k+1})$. COnsequentemente, $F_{2k-1}b = b'b = a^2 + 1 = F_{2k+1}^2 \Rightarrow b = F_{2k+3} \Rightarrow (a, b) = (F_{2k+1}, F_{2k+3}) \notin P$. Logo $P$ deve ser vazio.

**Exemplo 4.** *(URSS 1988) A sequência de inteiros $a_n$ é dada por $a_0 = 0$, $a_n = P(a_{n-1})$, onde $P(x)$ é um polinômio cujos coeficientes são inteiros positivos. Mostre que para quaisquer inteiros positivos $m, k$ com máximo divisor comum $d$, o máximo divisor comum de $a_m$ e $a_k$ é $a_d$.*

Quando temos um polinômio com coeficientes inteiros é sempre bom lembrar que $a - b \mid P(a) - P(b)$. Essa será nossa principal ferramenta nesta solução.

1. $a_m \mid a_{mr}$. Provaremos por indução. Se $a_{m(r-1)} \equiv 0 \pmod{a_m} \Rightarrow a_{m(r-1)+1} \equiv P(0) \pmod{a_m} \Rightarrow a_{m(r-1)+2} \equiv P(P(0)) \pmod{a_m} \Rightarrow a_{mr} = a_{m(r-1)+m} \equiv \underbrace{P(P(\ldots(P(0))}_{m\ vezes} = a_m \equiv 0 \pmod{a_m}$.

2. Se $l \mid a_t$ e $l \mid a_f \Rightarrow l \mid a_{t-f}$(Supondo $t > f$). (Deixaremos a prova dessa afirmação para o leitor).

Pelo teorema de Bezout, existem inteiros positivos $x, y$ tais que $mx - ky = d$. Seja $n = mdc(a_m, a_k)$. Como $n \mid a_m \mid a_{mx}$ e $n \mid a_k \mid a_{ky}$, pelo item 2, $n \mid a_{mx-ky} = a_d$. Mas $a_d \mid a_m$ e $a_d \mid a_k$, então $a_d \mid n$. Portanto $a_d = n$.

**Exemplo 5.** *Prove que existem infinitos números compostos n para os quais*

$$n \mid 3^{n-1} - 2^{n-1}.$$

Lema: $2^t \mid 3^{2^t} - 1\ \forall t \in \mathbb{N}$
Vamos provar o lema por indução. Para $t = 1$ é trivial. Suponha que a afirmação seja válida para $t = r$, provemos que também é válida para $t = r + 1$. Fatorando $2^{2^{t+1}} - 3^{3^{t+1}} = (2^{2^t} - 3^{3^t})(2^{2^t} + 3^{3^t})$, como o primeiro parêntesis é múltiplo de $2^t$ e o segundo é múltiplo de 2, o produto deles é múltiplo de $2^{t+1}$.

Seja $n = 3^{2^t} - 2^{2^t}$ com $t > 1$. Como $n - 1 \equiv (3^{2^t} - 1) - 2^{2^t} \equiv 0 \pmod{2^t}$, pelo lema, obtemos $n = 3^{2^t} - 2^{2^t} \mid 3^{n-1} - 2^{n-1}$. Aqui estamos usando o fato que $x^k - y^k \mid x^{mk} - y^{mk}$.

**Exemplo 6.** *Consideramos todas as sequências $(x_n)_{n\geq 1}$ de inteiros positivos satisfazendo*

$$x_{n+2} = \text{mdc}(x_n, x_{n+1}) + 2008, \quad \forall\, n \geq 1.$$

*Alguma dessas seqüências contém exatamente $10^{2008}$ números distintos?*

A idéia é construir a sequência de trás para frente. Mostraremos que para qualquer inteiro positivo $k > 1$, existe uma tal sequência contendo exatamente $k$ números distintos. Basta encontrarmos uma sequência que satisfaça:

$$x_{n+2} = \text{mdc}(x_n, x_{n+1}) + 2, \quad \forall\, n \geq 1. \ (1)$$

pois a multiplicação de todos os termos por 1004 produz a sequência do problema. Definamos $a_1 = 4, a_2 = 6, a_3 = 8, a_4 = 2(a_3 - 2)$ e $a_n = \dfrac{(a_{n-1} - 2)(a_{n-2} - 2)}{2}$ para $n \geq 5$.
É fácil ver por indução que todos os $a_i$ serão pares e que a sequência é crescente. Consequentemente, todos os $a_i$ com $i \geq 1$ são inteiros e distintos. Além disso, definamos os termos com índices não positivos por $a_{3k} = 4, a_{3k-1} = 6, a_{3k-2} = 4$ para $k \leq 0$.

$$\ldots a_6, a_5, a_4, a_3 = 8, a_2 = 6, a_1 = 4, a_0 = 4, a_{-1} = 6, a_{-2} = 4, a_{-3} = 4, a_{-4} = 6, \ldots$$

Afirmamos que a sequência anterior satisfaz $\text{mdc}(a_{n+2}, a_{n+1}) + 2 = a_n\ \forall n \in \mathbb{Z}$. É imediato verificar isso para $n \leq 1$ Para $n = 2$, $mdc(a_4, a_3) + 2 = mdc(12, 8) + 2 = 6 = a_2$. Para $n > 2$,

$$\text{mdc}(a_{n+2}, a_{n+1}) + 2 = \text{mdc}(\frac{(a_{n+1} - 2)(a_n - 2)}{2}, a_{n+1}) + 2 = \text{mdc}((a_{n+1})\frac{a_n - 2}{2} - a_n + 2, a_{n+1}) + 2$$

Portanto,

$$\text{mdc}(a_{n+2}, a_{n+1}) + 2 = \text{mdc}(a_n - 2, (a_n - 2)\frac{a_{n-1} - 2}{2}) + 2 = a_n - 2 + 2 = a_n.$$

Para encontrarmos uma sequência satisfazendo (1) com exatamente $k > 1$ termos distintos basta escolhermos $x_1 = a_k$ e $x_2 = a_{k-1}$ e definirmos o resto da sequência usando a relação de recorrência $x_{n+2} = \text{mdc}(x_n, x_{n+1}) + 2$

## Problemas Propostos

**Problema 7.** *Resolva em inteiros a equação:*

$$\frac{xy}{z} + \frac{xz}{y} + \frac{yz}{x} = 3$$

**Exemplo 8.** *Alguns inteiros positivos estão escritos no quadro. Podemos apagar quaisquer dois inteiros distintos e substituí-los pelo máximo divisor comum e o mínimo divisor comum dos dois números. Prove que eventualmente a operação de alterar os números não será mais executada.*

**Exemplo 9.** *Mostre que se $k > 1$ então $2^{k-1} \not\equiv -1 \pmod{k}$*

**Exemplo 10.** *(Estônia 2005) Sejam $a$, $b$ inteiros positivos primos entre si tais que $(a + b)/(a - b)$ é um inteiro positivo. Prove que ao menos um dentre os números $ab+1$ e $4ab+1$ é um quadrado perfeito.*

**Exemplo 11.** *(Ibero 1999) Seja $n$ um inteiro maior que 10 tal que cada um de seus dígitos pertence ao conjunto $S = \{1, 3, 7, 9\}$. Prove que $n$ tem algum divisor primo maior ou igual a 11.*