POTI
POLOS OLÍMPICOS DE TREINAMENTO INTENSIVO

Problemas Resolvidos

Nível 2

O Teorema Chinês dos Restos

Material elaborado por Valentino Amadeus Sichinel

Problemas

Problema 1. Encontre o menor inteiro positivo, com a exceção de $x = 1$, que satisfaz o seguinte sistema de congruências:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

Problema 2. Encontre todas as soluções do sistema:

$$\begin{aligned} 3x &\equiv 1 \pmod 4 \\ 2x &\equiv 1 \pmod 3 \\ 4x &\equiv 5 \pmod 7 \end{aligned}$$

Problema 3. Sejam $m_0, m_1, \ldots, m_r$ inteiros positivos dois a dois primos entre si. Mostre que existem $r+1$ inteiros consecutivos s, $s+1, \ldots, s+r$ tais que m_i divide $s+i$ para cada $i \in \{0, 1, \ldots, r\}$.

Problema 4. Sejam a e b inteiros positivos tais que $\text{mdc}(a, b) = 1$, e seja $c > 0$ um inteiro. Prove que existe um inteiro x tal que $\text{mdc}(a + bx, c) = 1$.

Problema 5. É verdade que, para cada n, $k \in \mathbb{N}$, existem n inteiros consecutivos tais que cada um é divisível pela k-ésima potência de algum primo?

Problema 6. Um ponto $(x, y) \in \mathbb{Z}^2$ é *legal* se $\text{mdc}(x, y) = 1$. Prove ou disprove: Dado um inteiro positivo n, existe um ponto $(a, b) \in \mathbb{Z}^2$ cuja distância a todo ponto legal é maior que n.

Problema 7. Demonstre que, dados k e n naturais, é possível encontrar n inteiros positivos consecutivos, cada um dos quais tem ao menos k fatores primos distintos.

Problema 8. Demonstre que, se a, b e c são três inteiros diferentes, existem infinitos inteiros positivos n para os quais $a+n$, $b+n$ e $c+n$ são primos relativos.

Problema 9. Demonstre que para todo inteiro positivo m e todo número par $2k$, este último pode ser escrito como a diferença de dois inteiros positivos, cada um dos quais é primo relativo com m.

Problema 10 (República Tcheca e Eslováquia)**.** Mostre que existe uma sequência crescente $\{a_n\}_{n=1}^{\infty}$ de números naturais tais que, para cada $k \geq 0$, a sequência $\{a_n + k\}_{n=1}^{\infty}$ contém uma quantidade finita de números primos.

Problema 11. Considere um inteiro $c \geq 1$ e a sequência $\{a_n\}_{n=1}^{\infty}$, definida por $a_1 = c$ e $a_{i+1} = c^{a_i}$. Mostre que essa sequência se torna eventualmente constante quando a reduzimos módulo n para algum inteiro $n > 1$ (isso significa que exite um j tal que $a_m \equiv a_j \pmod n$ para todo $m \geq j$).

Problema 12. Mostre que, para todo inteiro positivo n, existem inteiros positivos a e b tais que $4a^2 + 9b^2 - 1$ é divisível por n.

Problema 13 (EUA)**.** Seja n um inteiro positivo qualquer. Prove que existem n inteiros positivos $k_1, k_2, \ldots, k_n$ primos entre si, todos maiores que 1, tais que $k_1 k_2 \cdots k_n - 1$ é o produto de dois inteiros consecutivos.

Problema 14. Um inteiro é *livre de quadrados* se ele não é divisível pelo quadrado de nenhum número inteiro maior do que 1. Prove que existem intervalos arbitrariamente grandes de inteiros consecutivos, nenhum dos quais é livre de quadrados.

Soluções

1. Como $\text{mdc}(3,5) = \text{mdc}(5,7) = \text{mdc}(7,3) = 1$, o sistema apresentado admite exatamente uma solução módulo $3 \cdot 5 \cdot 7 = 105$. Como 1 é solução, concluímos que x é solução para o sistema se, e somente se, $x = 105k + 1$ para algum $k \in \mathbb{Z}$.

Dessa forma, o menor inteiro positivo, à exceção de 1, que satisfaz as três congruências dadas é $105 \cdot 1 + 1 = 106$.

2.

$$\text{Temos} \quad 3 \equiv -1 \pmod 4 \ , \ \text{donde} \quad 3^2 \equiv (-1)^2 \equiv 1 \pmod 4.$$

Assim,

$$3x \equiv 1 \pmod 4 \iff x \equiv 3 \pmod 4.$$

Da mesma forma,

$$2 \equiv -1 \pmod 3 \Rightarrow 2^2 \equiv (-1)^2 \equiv 1 \pmod 3,$$

donde

$$2x \equiv 1 \pmod 3 \iff x \equiv 2 \pmod 3.$$

Por fim, temos

$$4 \cdot 2 \equiv 1 \pmod 7$$

e, portanto,

$$4x \equiv 5 \pmod 7 \iff x \equiv 2 \cdot 5 \equiv 3 \pmod 7.$$

Dessa forma, o que queremos é resolver o sistema

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 7 \end{cases} \tag{1}$$

Como $\text{mdc}(4,7) = 1$, o sistema

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 3 \pmod 7 \end{cases}$$

possui exatamente uma solução módulo $4 \cdot 7 = 28$. É claro que essa solução é 3. Desse modo, se x é solução para o sistema original, então $x = 28k + 3$, para algum $k \in \mathbb{Z}$. Como

$$28k + 3 \equiv 2 \pmod 3 \iff k \equiv 2 \pmod 3,$$

x só é solução do sistema original se for da forma $28k + 3$, para algum k da forma $3q + 2$, isto é, se x for da forma $28(3q + 2) + 3 = 84q + 59$. Por outro lado, se $x = 84q + 59$ para algum $q \in \mathbb{Z}$, uma simples verificação mostra que x satisfaz as três congruências do sistema (1).

Concluímos, assim, que as soluções ao sistema apresentado no problema são exatamente os números da forma $84q + 59$, com $q \in \mathbb{Z}$.

3. Devemos mostrar que existe um inteiros s tal que

$$\begin{aligned} s &\equiv 0 \pmod{m_0} \\ s+1 &\equiv 0 \pmod{m_1} \\ &\vdots \\ s+r &\equiv 0 \pmod{m_r} \end{aligned}$$

Isso é o mesmo que mostrar que existe um inteiro s tal que

$$\begin{aligned} s &\equiv 0 \pmod{m_0} \\ s &\equiv -1 \pmod{m_1} \\ &\vdots \\ s &\equiv -r \pmod{m_r} \end{aligned}$$

Como $m_0, m_1, \ldots, m_r$ são dois a dois primos entre si, o teorema chinês dos restos garante a existência de um tal inteiro s. Isso conclui, então, a solução.

4. Queremos um inteiro x tal que

$$a + bx \not\equiv 0 \pmod{p} \quad \forall \ p \text{ primo tal que } p \mid c.$$

Para os primos p tais que $p \mid b$, qualquer x basta: se $p \mid b$, $a+bx \equiv a \pmod{p}$ e, como $\text{mdc}(a,\, b) = 1$, se $p \mid b$, então $p \nmid a$.

Sejam, então, $p_1, p_2, \ldots, p_k$ os fatores primos de c que não dividem b. Queremos mostrar que existe $x \in \mathbb{Z}$ tal que

$$\begin{aligned} a + bx &\not\equiv 0 \pmod{p_1} \\ a + bx &\not\equiv 0 \pmod{p_2} \\ &\vdots \\ a + bx &\not\equiv 0 \pmod{p_k} \end{aligned}$$

É claro que é suficiente encontrarmos x tal que

$$\begin{aligned} a + bx &\equiv 1 \pmod{p_1} \\ a + bx &\equiv 1 \pmod{p_2} \\ &\vdots \\ a + bx &\equiv 1 \pmod{p_k} \end{aligned} \tag{1}$$

E essa tarefa pode ser facilmente resolvida com o teorema Chinês dos restos.

Se q_i é o inverso de b módulo p_i (isto é, $b \cdot q_i \equiv 1 \pmod{p_i}$) para $i = 1, 2, \ldots, k$, o sistema (1), que é equivalente a

$$\begin{aligned} bx &\equiv 1 - a \pmod{p_1} \\ bx &\equiv 1 - a \pmod{p_2} \\ &\vdots \\ bx &\equiv 1 - a \pmod{p_k} \end{aligned}$$

, é equivalente a

$$\begin{aligned} x &\equiv q_1(1-a) \pmod{p_1} \\ x &\equiv q_2(1-a) \pmod{p_2} \\ &\vdots \\ x &\equiv q_k(1-a) \pmod{p_k} \end{aligned}$$

que, pelo teorema Chinês dos restos, tem solução.

Dessa forma, existe $x \in \mathbb{Z}$ tal que $a + bx$ não é divisível por nenhum primo que divide c, isto é, tal que $\text{mdc}(a + bx,\, c) = 1$.

5. Sim. Vejamos por que.

Dados n, k naturais, o que queremos é encontrar $m \in \mathbb{Z}$ e primos $p_1, p_2, \ldots, p_n$ tais que $p_i^k \mid m + i \quad \forall\, i \in \{1, 2, \ldots, n\}$. Em outras palavras, queremos encontrar m e $p_1, p_2, \ldots, p_k$ tais que

$$\begin{aligned} m &\equiv -1 \pmod{p_1^k} \\ m &\equiv -2 \pmod{p_2^k} \\ &\vdots \\ m &\equiv -n \pmod{p_n^k} \end{aligned}$$

Isso é evidentemente possível, segundo o teorema Chinês dos restos, bastando que escolhamos primos $p_1, p_2, \ldots, p_k$ distintos entre si. De fato, se $p_i \neq p_j$ e p_i e p_j são primos, então $\text{mdc}(p_i,\, p_j) = 1$.

6. Vamos provar que existem, de fato, pontos arbitrariamente isolados dos pontos legais.

Seja, então, $n \in \mathbb{N}$. Queremos $a, b \in \mathbb{Z}$ tais que $\text{mdc}(p,\, q) \neq 1$, sejam quais forem $p \in \{a - n, \ldots, a + n\}$ e $q \in \{b - n, \ldots, b + n\}$.

Para tanto, faremos o seguinte: para cada par $(i,\, j) \in \{-n, \ldots, n\} \times \{-n, \ldots, n\}$, escolheremos um primo $p_{i,j}$, responsável por assegurar que $a+i$ e $b+j$ não serão em primos entre si. Em outras palavras, escolhemos $(2n + 1)^2$ primos $p_{i,j}$ distintos, um para cada par $(i,\, j) \in \{-n, \ldots, n\} \times \{-n, \ldots, n\}$ e, então, encontramos $a, b \in \mathbb{Z}$ tais que $p_{i,j} \mid a + i$ e $p_{i,j} \mid b + j$, para todos i, j.

Essa é uma simples tarefa para o teorema Chinês dos restos: uma vez escolhidos os primos $p_{i,j}$, dois a dois distintos, tudo de que precisamos é ter

$$a \equiv -i \pmod{p_{i,j}} \quad \forall \quad (i,\, j) \in \{-n, \ldots, n\} \times \{-n, \ldots, n\}$$

e

$$b \equiv -j \pmod{p_{i,j}} \quad \forall \quad (i,\, j) \in \{-n, \ldots, n\} \times \{-n, \ldots, n\}.$$

E isso certamente é possível, de acordo com o teorema.

Dessa forma, existem inteiros a, b tais que, se $p \in \{a - n, \ldots, a + n\}$ e $q \in \{b - n, \ldots, b + n\}$, então $\text{mdc}(p,\, q) > 1$. Para tais a e b, temos que $(x,\, y)$ ser legal implica $|x - a| > n$ e $|y - b| > n$, o que implica $\sqrt{(x-a)^2 + (y-b)^2} > n\sqrt{2} > n$ e, portanto, $(a,\, b)$ está a uma distância maior que n de qualquer ponto legal.

7. Sejam k e n números naturais quaisquer.

Queremos mostrar que existem números primos $p_{i,j}$, um para cada par $(i,\, j) \in \{1, \ldots, n\} \times \{1, \ldots, k\}$, sendo p_{i,j_1} distinto de p_{i,j_2} para $j_1 \neq j_2$, e um número inteiro positivo a, tais que $a + i$ é divisível por $p_{i,j}$, para todos $1 \leq i \leq n$ e $1 \leq j \leq k$.

Se fizermos isso, teremos n números inteiros positivos consecutivos, $a+1, a+2, \ldots, a+n$, tais que cada um dos quais possui ao menos k fatores primos distintos: $a + i$ é divisível por $p_{i,1}$, por $p_{i,2}$, ..., e por $p_{i,k}$.

Mais uma tarefa simples para o teorema Chinês dos restos.

Podemos escolher primos $p_{i,j}$ quaisquer (distintos dois a dois; um para cada par $(i,\, j)$), e tudo de que precisamos é assegurar que

$$\begin{aligned} a + 1 &\equiv 0 \pmod{p_{1,j}} \quad \forall\, j \in \{1, \ldots, k\} \\ a + 2 &\equiv 0 \pmod{p_{2,j}} \quad \forall\, j \in \{1, \ldots, k\} \\ &\vdots \\ a + n &\equiv 0 \pmod{p_{n,j}} \quad \forall\, j \in \{1, \ldots, k\} \end{aligned}$$

, isto é, que

$$a \equiv -i \pmod{p_{i,j}} \quad \forall\ (i,\, j) \in \{1, \ldots, n\} \times \{1, \ldots, k\}.$$

O teorema Chinês dos restos nos garante que um tal número a existe, uma vez que escolhemos os primos $p_{i,j}$ distintos dois a dois.

8. Sejam a, b e c inteiros positivos distintos. Para qualquer $n \in \mathbb{N}$, $\text{mdc}(a+n,\, b+n) = \text{mdc}(a+n,\, b-a)$. Assim, para que tenhamos $\text{mdc}(a + n,\, b + n) = 1$, basta que tenhamos $a + n \not\equiv 0 \pmod{p}$ para todos os primos p que dividem $b - a$. Em outras palavras, se $p_1, p_2, \ldots, p_k$ são os fatores primos de $b - a$, temos $\text{mdc}(a + n,\, b + n) = 1$ se, e somente se,

$$\begin{aligned} n &\not\equiv -a \pmod{p_1} \\ n &\not\equiv -a \pmod{p_2} \\ &\vdots \\ n &\not\equiv -a \pmod{p_k} \end{aligned}$$

De modo análogo, se $q_1, q_2, \ldots, q_l$ são os fatores primos de $c-b$, e $r_1, r_2, \ldots, r_t$ são os fatores primos de $a - c$, então $\text{mdc}(b + n,\, c + n) = 1$ se, e somente se,

$$\begin{aligned} n &\not\equiv -b \pmod{q_1} \\ n &\not\equiv -b \pmod{q_2} \\ &\vdots \\ n &\not\equiv -b \pmod{q_l} \end{aligned}$$

, e $\text{mdc}(c + n,\, a + n) = 1$ se, e somente se,

$$\begin{aligned} n &\not\equiv -c \pmod{r_1} \\ n &\not\equiv -c \pmod{r_2} \\ &\vdots \\ n &\not\equiv -c \pmod{r_t} \end{aligned}$$

Por simplicidade, vamos chamar os primos que dividem $b-a$ ou $c-b$ ou $a-c$ de $s_1, s_2, \ldots, s_m$. Pelo teorema Chinês dos restos, é suficiente encontrarmos, para cada primo s_i, um resíduo x_i tal que

$$x_i \not\equiv \begin{cases} -a & \text{se } s_i \mid b-a \\ -b & \text{se } s_i \mid c-b \\ -c & \text{se } s_i \mid a-c \end{cases} \pmod{s_i} \tag{1}$$

Parece simples, mas temos um empecilho: pode ser que s_i divida mais de uma das diferenças. E se s_i for 2 ou 3, isso causaria um problema, já que só temos dois resíduos possíveis módulo 2, e três módulo 3. Felizmente, se s_i divide duas das diferenças, então $-a \equiv -b \equiv -c \pmod{s_i}$. De fato, se $s_i \mid b-a$, por exemplo, então $b-a \equiv 0 \pmod{s_i} \Rightarrow -a \equiv -b \pmod{s_i}$ e, de modo análogo, uma diferença envolvendo c é suficiente para concluir que $-c \equiv -a \pmod{s_i}$ ou $-c \equiv -b \pmod{s_i}$. Dessa forma, podemos sempre escolher x_i tal que (1) é satisfeito. Após efetuarmos tais escolhas, tudo de que precisamos para que $a+n$, $b+n$ e $c+n$ sejam primos entre si é que

$$\begin{aligned} n &\equiv x_1 \pmod{s_1} \\ n &\equiv x_2 \pmod{s_2} \\ &\vdots \\ n &\equiv x_m \pmod{s_m} \end{aligned}$$

De acordo com o teorema Chinês dos restos, existe um resíduo n_0 módulo $P = \prod_{i=1}^{m} s_i$ tal que $PK+n_0$ satisfaz tais condições, seja qual for $K \in \mathbb{Z}$. Portanto, todo número n da forma $n = PK+n_0$, com K inteiro positivo, é um inteiro positivo tal que $a+n$, $b+n$ e $c+n$ são primos relativos e, dessa forma, tais inteiros existem em quantidade infinita.

9. Primeiro, vamos mostrar que existem inteiros positivos a e b, primos relativos com m, tais que $a-b \equiv 2k \pmod{m}$.

Para tanto, escrevamos $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_l^{\alpha_l}$, a decomposição em fatores primos de m, e consideremos $i \in \{1, \ldots, l\}$ qualquer. Afirmo que existem x_i e y_i tais que $x_i \not\equiv 0 \pmod{p_i^{\alpha_i}}$, $y_i \not\equiv 0 \pmod{p_i^{\alpha_i}}$ e $x_i - y_i \equiv 2k \pmod{p_i^{\alpha_i}}$. Vejamos por que.

Se $2k \equiv 0 \pmod{p_i^{\alpha_i}}$, basta considerarmos $x_i = y_i = 1$.

Se $2k \not\equiv 0 \pmod{p_i^{\alpha_i}}$, $p_i^{\alpha_i} > 2$ (pois $2k \equiv 0 \pmod 2$) e, assim, existem ao menos três resíduos distintos módulo $p_i^{\alpha_i}$. Em particular, existe um resíduo que não é congruente a 0 nem a $2k$. Se chamarmos esse resíduo de x_i, podemos tomar $y_i = 2k - x_i$, e as condições serão satisfeitas.

Existem, portanto, para cada $i \in \{1, \ldots, l\}$, x_i e y_i tais que $x_i \not\equiv 0 \pmod{p_i^{\alpha_i}}$, $y_i \not\equiv 0 \pmod{p_i^{\alpha_i}}$ e $x_i - y_i \equiv 2k \pmod{p_i^{\alpha_i}}$. Pelo teorema chinês dos restos, existem a e b tais que

$$\begin{aligned} a &\equiv x_1 \pmod{p_1^{\alpha_1}} \\ a &\equiv x_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ a &\equiv x_l \pmod{p_l^{\alpha_l}} \end{aligned}$$

e

$$\begin{aligned} b &\equiv y_1 \pmod{p_1^{\alpha_1}} \\ b &\equiv y_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ b &\equiv y_l \pmod{p_l^{\alpha_l}} \end{aligned}$$

Em função das condições sob as quais encontramos os x_i's e os y_i's, tais inteiros a e b são primos relativos com $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_l^{\alpha_l} = m$, e são tais que $a - b \equiv 2k \pmod{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_l^{\alpha_l} = m}$.

Temos, então, inteiros a e b tais que $\text{mdc}(a, m) = \text{mdc}(b, m) = 1$ e $a - b = mq + 2k$ para algum $q \in \mathbb{Z}$. Se fizermos $b' = b + mq$, ficamos com inteiros a e b', primos relativos com m, cuja diferença é igual a $2k$.

Ainda não terminamos. Precisamos que os inteiros sejam positivos. Mas isso é simples: certamente, $a+m(|a|+|b|) > 0$ e $b'+m(|a|+|b'|) > 0$. Esses dois novos números, $a+m(|a|+|b|)$ e $b'+m(|a|+|b'|)$, são então inteiros positivos. Como cada um deles é um múltiplo de m somado a a ou a b', eles são ainda primos relativos com m. Como o múltiplo que somamos em ambos é o mesmo, a diferença desses dois novos números é igual a $a - b'$, que é igual a $2k$. Isso encerra a demonstração.

10. Sejam $p_0, p_1, p_2, \ldots$ os números primos (todos eles: $2, 3, 5, \ldots$). Sim, começamos a indexação por 0. O motivo ficará claro em breve.

Em um certo sentido, o k-ésimo número primo será responsável por evitar que a sequência $\{a_n + k\}_{n=1}^{\infty}$ tenha infinitos primos.

Definiremos a sequência $\{a_n\}_{n=1}^{\infty}$ indutivamente.

Começamos por escolher $a_1 \in \mathbb{N}$ tal que $a_1 + 0 \equiv 0 \pmod{p_0}$.

Depois, escolhemos $a_2 \in \mathbb{N}$ tal que $a_2 + 0 \equiv 0 \pmod{p_0}$, $a_2 + 1 \equiv 0 \pmod{p_1}$ e $a_2 > a_1$. Veja que isso pode ser feito: pelo teorema chinês dos restos, existe x tal que todo número da forma $p_0p_1q + x$ satisfaz as congruências; basta, então, escolher q grande o suficiente para que tenhamos $p_0p_1q+x > a_1$.

De uma forma geral, quando nos concentrarmos em escolher o n-ésimo termo da sequência, já teremos escolhido $a_1, a_2, \ldots, a_{n-1}$, e poderemos, então, tomar um natural a_n tal que

$$\begin{aligned} a_n + 0 &\equiv 0 \pmod{p_0} \\ a_n + 1 &\equiv 0 \pmod{p_1} \\ &\vdots \\ a_n + n - 1 &\equiv 0 \pmod{p_{n-1}} \end{aligned}$$

e $a_n > a_{n-1}$. De fato, pelo teorema chinês dos restos, existe x tal que todo número da forma $p_0p_1 \cdots p_{n-1}q + x$ satisfaz as congruências acima. Tomando q grande o suficiente, teremos $p_0p_1 \cdots p_{n-1}q + x > a_{n-1}$ e, então, podemos fazer $a_n = p_0p_1 \cdots p_{n-1}q + x$.

Seguindo esse procedimento, definimos uma sequência crescente $\{a_n\}_{n=1}^{\infty}$ de números naturais tais que, para todo i,

$$\begin{aligned} a_i + 0 &\equiv 0 \pmod{p_0} \\ a_i + 1 &\equiv 0 \pmod{p_1} \\ &\vdots \\ a_i + i - 1 &\equiv 0 \pmod{p_{i-1}} \end{aligned}$$

Se assim o fizermos, para cada $k \geq 0$, a sequência $\{a_n+k\}_{n=1}^{\infty}$ será tal que, a partir do $(k+1)$-ésimo (a saber, $a_{k+1} + k$), todos os termos são divisíveis por p_k. Como a sequência é crescente, no máximo um desses termos é igual a p_k e, assim, todos os demais são compostos.

Dessa forma, para cada $k \geq 0$, a sequência $\{a_n + k\}_{n=1}^{\infty}$ contém no máximo $k + 1$ números primos.

11. Se $c = 1$, a sequência toda é constante (igual a 1). Suponhamos, então, que $c > 1$.

Provaremos por indução que, para cada $n \in \mathbb{N}$ maior que 1, existe um índice j a partir do qual a sequência $\{a_i\}_{i=1}^{\infty}$ é constante módulo n.

A **base** ($n = 2$) é simples: se c é ímpar, $a_i \equiv 1 \pmod{2}$ $\forall i$ e, se c é par, $a_i \equiv 0 \pmod{2}$ $\forall i$.

Suponhamos, então, que para todo $n' < n$ existe um índice j' a partir do qual $\{a_i\}_{i=1}^{\infty}$ é constante módulo n', isto é, tal que $a_m \equiv a_{j'} \pmod{n'}$ para todo $m \geq j'$. Essa é a **hipótese de indução**.

Vamos, agora, ao **passo indutivo**, isto é, vamos mostrar que o resultado é válido para n também.

Se $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, a fatoração em primos de n, for tal que $k \geq 2$, não há muito que fazer. De fato, nesse caso, $p_i^{\alpha_i} < n$ para todo $i \in \{1, \ldots, k\}$ e assim, pela hipótese de indução, existe, para cada $i \in \{1, \ldots, k\}$, um j_i tal que $a_m \equiv a_{j_i} \pmod{p_i^{\alpha_i}}$ $\forall m \geq j_i$. Se fizermos $j := \max(j_1, j_2, \ldots, j_k)$, teremos

$$\begin{aligned} a_m &\equiv a_j \pmod{p_1^{\alpha_1}} \\ a_m &\equiv a_j \pmod{p_2^{\alpha_2}} \\ &\vdots \\ a_m &\equiv a_j \pmod{p_k^{\alpha_k}} \end{aligned}$$

para todo $m \geq j$, e o teorema chinês dos restos nos assegura que, nesse caso,

$$a_m \equiv a_j \pmod{n}$$

(para todo $m \geq j$).

Dessa forma, é suficiente que consideremos o caso em que n é uma potência de primo. Suporemos, então, que $n = p^{\alpha}$, para algum primo p.

Como $c > 1$, $\{a_i\}_{i=1}^{\infty}$ é crescente. Logo, existe j tal que $a_i > \alpha$ para todo $i \geq j$. Como $a_{i+1} = c^{a_i}$, segue daí que, se $p \,|\, c$, então $p^{\alpha} \,|\, a_{i+1}$ para todo $i \geq j$. Assim, nesse caso, $a_{i+1} \equiv 0 \pmod{p^{\alpha}}$ para todo $i \geq j$. Resta considerarmos, então, o caso em que $p \nmid c$.

Observe que $\phi(p^{\alpha}) < p^{\alpha}$. Assim, pela hipótese de indução, existe j' tal que $a_m \equiv a_{j'} \pmod{\phi(p^{\alpha})}$ para todo $m \geq j'$. Se $p \nmid c$, $\text{mdc}(c, p^{\alpha}) = 1$ e, assim, vem daí que $c^{a_m - a_{j'}} \equiv 1 \pmod{p^{\alpha}}$ para todo $m \geq j'$. Em outras palavras, $c^{a_m} \equiv c^{a_{j'}} \pmod{p^{\alpha}}$ para todo $m \geq j'$, ou seja, $a_{m+1} \equiv a_{j'+1} \pmod{p^{\alpha}}$ para todo $m \geq j'$. Fazendo $j = j' + 1$, concluímos que, nesse caso, $a_m \equiv a_j \pmod{n = p^{\alpha}}$ para todo $m \geq j$.

Isso conclui o passo indutivo, e o princípio de indução finita conclui nossa demonstração.

12. Escrevamos $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, a fatoração em primos de n.

Se, para cada $i \in \{1, \ldots, k\}$, encontrarmos a_i e b_i tais que $4a_i^2 + 9b_i^2 - 1$ é divisível por $p_i^{\alpha_i}$, será suficiente que encontremos a e b tais que

$$\begin{aligned} a &\equiv a_1 \pmod{p_1^{\alpha_1}} \\ a &\equiv a_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ a &\equiv a_k \pmod{p_k^{\alpha_k}} \end{aligned}$$

e

$$\begin{aligned} b &\equiv b_1 \pmod{p_1^{\alpha_1}} \\ b &\equiv b_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ b &\equiv b_k \pmod{p_k^{\alpha_k}} \end{aligned}$$

Mas isso é simples: como $\text{mdc}(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ para quaisquer $i \neq j$, o teorema chinês dos restos nos garante a existência de tais a e b.

Vamos, então, considerar uma potência de primo p^α qualquer, e mostrar que existem a e b tais que p^α divide $4a^2 + 9b^2 - 1$. Dividiremos a solução em dois casos:

- Se $p = 2$, basta tomarmos $a \equiv 0 \pmod{2^\alpha}$ e $b \equiv 3^{-1} \pmod{2^\alpha}$ (3^{-1} é o inverso de 3 módulo 2^α).
- Se $p \neq 2$, basta tomarmos $a \equiv 2^{-1} \pmod{p^\alpha}$ e $b \equiv 0 \pmod{p^\alpha}$ (2^{-1} é o inverso de 2 módulo p^α).

13. $k_1k_2\cdots k_n - 1$ ser o produto de dois inteiros consecutivos equivale à existência de um inteiro a tal que

$$k_1k_2\cdots k_n - 1 = a(a+1),$$

isto é, tal que

$$a(a+1) + 1 = k_1k_2\cdots k_n.$$

Dessa forma, a existência de inteiros positivos $k_1, k_2, \ldots, k_n$ primos entre si, todos maiores que 1, tais que $k_1k_2\cdots k_n - 1$ é o produto de dois inteiros consecutivos equivale à existência de um inteiro a tal que $a(a+1)+1$ possui ao menos n fatores primos distintos.

Assim, se encontrarmos n primos distintos $p_1, p_2, \ldots, p_n$ e n inteiros $a_1, a_2, \ldots, a_n$ tais que

$$a_i(a_i+1) + 1 \equiv 0 \pmod{p_i} \quad \forall\ i \in \{1, \ldots, n\},$$

teremos resolvido o problema. De fato, pelo teorema chinês dos restos, existe, nesse caso, um inteiro a tal que

$$\begin{aligned} a &\equiv a_1 \pmod{p_1} \\ a &\equiv a_2 \pmod{p_2} \\ &\vdots \\ a &\equiv a_n \pmod{p_n} \end{aligned}$$

e, portanto, tal que

$$a(a+1) + 1 \equiv 0 \pmod{p_i} \quad \forall\ i \in \{1, \ldots, n\}.$$

É suficiente que mostremos, então, que a quantidade de números primos que divide algum número da forma $a(a+1)+1$ é pelo menos n. Vamos mostrar que, de fato, existem infinitos números primos que dividem algum número da forma $a(a+1)+1$.

Suponhamos, por absurdo, que existe apenas uma quantidade finita de tais números primos, e chamemos esses números primos de $p_1, p_2, \ldots, p_k$. Se $P := p_1p_2\cdots p_k$,

$$P(P+1) + 1 \equiv 1 \not\equiv 0 \pmod{p_i} \quad \forall\ i \in \{1, \ldots, k\}.$$

Mas $P(P+1)+1$ não é igual a 1, já que $P(P+1) \neq 0$ e, portanto, deve ser divisível por algum número primo. Absurdo!

Dessa forma, há de haver infinitos primos que dividem algum número da forma $a(a+1)+1$. Isso completa a solução.

14. Devemos mostrar que, dado um inteiro positivo n qualquer, existem n inteiros consecutivos $a+1, a+2, \ldots, a+n$, nenhum dos quais é livre de quadrados.

Para garantirmos que um número não é livre de quadrados, basta que garantamos que ele é divisível pelo quadrado de algum número primo. Dessa forma, para atingirmos nosso objetivo, basta que encontremos um número inteiro a e n números primos $p_1, p_2, \ldots, p_n$ tais que

$$\begin{aligned} a+1 &\equiv 0 \pmod{p_1^2} \\ a+2 &\equiv 0 \pmod{p_2^2} \\ &\vdots \\ a+n &\equiv 0 \pmod{p_n^2} \end{aligned}$$

isto é, tais que

$$\begin{aligned} a &\equiv -1 \pmod{p_1^2} \\ a &\equiv -2 \pmod{p_2^2} \\ &\vdots \\ a &\equiv -n \pmod{p_n^2} \end{aligned}$$

Isso é garantidamente possível, de acordo com o teorema chinês dos restos, bastando para tanto que escolhamos primos $p_1, p_2, \ldots, p_n$ distintos entre si.

Dessa forma, para cada inteiro n, existe um intervalo de ao menos n inteiros consecutivos, nenhum dos quais é livre de quadrados.