POTI
POLOS OLÍMPICOS DE TREINAMENTO INTENSIVO

Problemas Resolvidos

Nível 2

Congruências III

Material elaborado por Valentino Amadeus Sichinel

Problemas

Problema 1. Determine os dois últimos algarismos de:

(a) 3^{1000}

(b) 13^{100}

(c) 17^{2020}

(d) $7^{7^{1000}}$

Problema 2. Prove que $504 \mid n^9 - n^3$, seja qual for $n \in \mathbb{N}$.

Problema 3. Seja n um inteiro positivo ímpar que não é divisível por 5. Mostre que existe um número da forma 111...11 que é divisível por n.

Problema 4 (OBM)**.** Mostre que existem infinitos números da forma 1999...91 que são divisíveis por 1991.

Problema 5. Seja $n > 1$ um inteiro. Prove que

$$\sum_{\substack{0<a<n \\ \text{mdc}(a,n)=1}} a \;=\; \frac{n\phi(n)}{2}.$$

Problema 6. Sejam m e n inteiros maiores que 1 tais que $\text{mdc}(m,\, n) = 1$. Mostre que

$$m^{\phi(n)} + n^{\phi(m)} \;\equiv\; 1 \pmod{mn}.$$

Problema 7. Seja n um inteiro maior que 4 tal que tanto $n-1$ quanto $n+1$ são primos. Mostre que

$$\phi(n) \;\leq\; \frac{n}{3}.$$

Problema 8. Seja n um inteiro positivo. Prove que

$$\sum_{d \,|\, n} \phi(d) \;=\; n.$$

Problema 9. Mostre que existe um natural n tal que $2^n > 10^{2000}$ e tal que 2^n possui, entre suas últimas 2000 casas decimais, ao menos 1000 zeros consecutivos.

Problema 10. Prove que para cada número natural k existe ao menos um número natural n tal que

$$\phi(n+k) \;=\; \phi(n).$$

Dica: Considere o menor primo p que não divide k e olhe para o número $n = (p-1)k$.

Problema 11 (EUA)**.** Seja n um número inteiro maior que 1. Mostre que a sequência

$$2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \ldots \pmod{n}$$

é eventualmente constante, isto é, a partir de um certo termo da sequência, todos os termos deixam o mesmo resto quando divididos por n.

Problema 12. Mostre que, para qualquer inteiro positivo n distinto de 2 e de 6,

$$\phi(n) \;\geq\; \sqrt{n}.$$

Problema 13. Para quantos inteiros $1 \leq i \leq 1000$ existe um inteiro $1 \leq j \leq 1000$ tal que $i \mid 2^j - 1$?

Problema 14. Mostre que existem infinitos números da forma 2000...021 que são divisíveis por 2021.

Soluções

1. (a) Para encontrar os dois últimos dígitos de 3^{1000}, é necessário e suficiente que encontremos o resto da divisão de 3^{1000} por 100.

Como $\text{mdc}(3,\ 100) = 1$, o Teorema de Euler nos diz que $3^{\phi(100)} \equiv 1 \pmod{100}$.

Como $100 = 2^2 \cdot 5^2$, $\phi(100) = 1 \cdot 2^1 \cdot 4 \cdot 5^1 = 40$. Assim, $3^{40} \equiv 1 \pmod{100}$.

Dessa forma,

$$3^{1000} \equiv 3^{40 \cdot 25} \equiv (3^{40})^{25} \equiv 1^{25} \equiv 1 \pmod{100}.$$

Portanto, os dois últimos algarismos de 3^{1000} são 0 e 1, nessa ordem.

(b) Para encontrar os dois últimos dígitos de 13^{100}, é necessário e suficiente que encontremos o resto da divisão de 13^{100} por 100.

Como $\text{mdc}(13,\ 100) = 1$, o Teorema de Euler nos diz que $13^{\phi(100)} \equiv 1 \pmod{100}$.

Como $100 = 2^2 \cdot 5^2$, $\phi(100) = 1 \cdot 2^1 \cdot 4 \cdot 5^1 = 40$. Assim, $13^{40} \equiv 1 \pmod{100}$.

Dessa forma,

$$13^{100} \equiv 13^{40 \cdot 2 + 20} \equiv (13^{40})^2 \cdot 13^{20} \equiv 1^2 \cdot 13^{20} \equiv 1 \cdot 13^{20} \equiv 13^{20} \pmod{100}.$$

Uma conta simples mostra que

$$13^3 \equiv 169 \cdot 13 \equiv 69 \cdot 13 \equiv 897 \equiv 97 \equiv -3 \pmod{100}.$$

Logo,

$$13^{20} \equiv 13^{3 \cdot 6 + 2} \equiv (13^3)^6 \cdot 13^2 \equiv (-3)^6 \cdot 13^2 \equiv 729 \cdot 169 \equiv 29 \cdot 69 \equiv 2001 \equiv 1 \pmod{100}.$$

Portanto, os dois últimos algarismos de 13^{100} são 0 e 1, nessa ordem.

(c) Para encontrar os dois últimos dígitos de 17^{2020}, é necessário e suficiente que encontremos o resto da divisão de 17^{2020} por 100.

Como $\text{mdc}(17,\ 100) = 1$, o Teorema de Euler nos diz que $17^{\phi(100)} \equiv 1 \pmod{100}$.

Como $100 = 2^2 \cdot 5^2$, $\phi(100) = 1 \cdot 2^1 \cdot 4 \cdot 5^1 = 40$. Assim, $17^{40} \equiv 1 \pmod{100}$.

Dessa forma,

$$17^{2020} \equiv 17^{40 \cdot 50 + 20} \equiv (17^{40})^{50} \cdot 17^{20} \equiv 1^{50} \cdot 17^{20} \equiv 17^{20} \pmod{100}.$$

E agora? Os restos que as primeiras potências de 17 deixam quando divididas por 100 parecem grandes demais para que tentemos simplificar $17^{20} \pmod{100}$... O truque está em olhar módulo 4 e módulo 25 separadamente:

Temos $\text{mdc}(17, 4) = 1$ e, portanto,

$$17^{20} \equiv 17^{2 \cdot 10} \equiv (17^2)^{10} \equiv (17^{\phi(4)})^{10} \equiv 1^{10} \equiv 1 \pmod{4},$$

ou seja, $4 \mid 17^{20} - 1$.

Por outro lado, $\text{mdc}(17, 25) = 1$ e, portanto,

$$17^{20} \equiv 17^{\phi(25)} \equiv 1 \pmod{25},$$

ou seja, $25 \mid 17^{20} - 1$.

Como tanto 4 quanto 25 dividem $17^{20} - 1$, e como $\text{mdc}(4, 25) = 1$, segue que $4 \times 25 = 100$ divide $17^{20} - 1$. Daí, $17^{20} \equiv 1 \pmod{100}$.

Portanto, os dois últimos algarismos de 17^{2020} são 0 e 1, nessa ordem.

(d) Para encontrar os dois últimos dígitos de $7^{7^{1000}}$, é necessário e suficiente que encontremos o resto da divisão de $7^{7^{1000}}$ por 100.

Como mdc(7, 100) = 1, o Teorema de Euler nos diz que $7^{\phi(100)} \equiv 1 \pmod{100}$.

Como $100 = 2^2 \cdot 5^2$, $\phi(100) = 1 \cdot 2^1 \cdot 4 \cdot 5^1 = 40$. Assim, $7^{40} \equiv 1 \pmod{100}$.

É útil, então, que decomponhamos 7^{1000} como soma de um múltiplo de 40 e um resto.

Veja que $7^2 \equiv 49 \equiv 9 \pmod{40}$. Assim, $7^4 \equiv 9^2 \equiv 81 \equiv 1 \pmod{40}$. Daí,

$$7^{1000} \equiv (7^4)^{250} \equiv 1^{250} \equiv 1 \pmod{40}.$$

Isso implica a existência de um inteiro positivo k tal que $7^{1000} = 40 \cdot k + 1$. Dessa forma,

$$7^{7^{1000}} \equiv 7^{40 \cdot k + 1} \equiv (7^{40})^k \cdot 7 \equiv 1^k \cdot 7 \equiv 7 \pmod{100}.$$

Portanto, os dois últimos algarismos de $7^{7^{1000}}$ são 0 e 7, nessa ordem.

2. O primeiro passo é fatorar 504: $504 = 2^3 \cdot 3^2 \cdot 7$. Como 2^3, 3^2 e 7 são dois a dois primos entre si, para mostrar que $504 \mid n^9 - n^3$, é necessário e suficiente que mostremos que $2^3 \mid n^9 - n^3$, que $3^2 \mid n^9 - n^3$, e que $7 \mid n^9 - n^3$.

Comecemos pelo 2^3.

Se $n \equiv 0 \pmod 2$, $n^9 - n^3 = n^3(n^6 - 1) \equiv 0 \pmod{2^3}$.

Por outro lado, se $n \not\equiv 0 \pmod 2$, então $\text{mdc}(n, 2^3) = 1$. Daí, $n^2 \equiv 1 \pmod{2^3}$[1]. Logo, $n^9 - n^3 \equiv (n^2)^4 \cdot n - n^2 \cdot n \equiv n - n \equiv 0 \pmod{2^3}$.

Dessa forma, em qualquer caso, $2^3 \mid n^9 - n^3$.

Analisemos a divisibilidade por 3^2.

Se $n \equiv 0 \pmod 3$, $n^9 - n^3 = n^2(n^7 - n) \equiv 0 \pmod{3^2}$.

Por outro lado, se $n \not\equiv 0 \pmod 3$, então $\text{mdc}(n, 3^2) = 1$. Daí, pelo Teorema de Euler, $n^6 \equiv 1 \pmod{3^2}$ (de fato, $\phi(3^2) = 6$). Logo, $n^9 - n^3 \equiv n^3(n^6 - 1) \equiv n^3(1 - 1) \equiv 0 \pmod{3^2}$.

Dessa forma, em qualquer caso, $3^2 \mid n^9 - n^3$.

Por fim, se $n \equiv 0 \pmod 7$, então $n^9 - n^3 = n(n^8 - n^2) \equiv 0 \pmod 7$ e, se $n \not\equiv 0 \pmod 7$, o Teorema de Euler nos dá $n^6 \equiv 1 \pmod 7$, donde $n^9 - n^3 = n^3(n^6 - 1) \equiv n^3(1 - 1) \equiv 0 \pmod 7$. Dessa forma, em qualquer caso, $7 \mid n^9 - n^3$.

Como $n^9 - n^3$ é divisível por 2^3, por 3^2 e por 7, independentemente do valor de n, concluímos que $504 = 2^3 \cdot 3^2 \cdot 7 \mid n^9 - n^3$, seja qual for $n \in \mathbb{N}$.

3. Antes de mais nada, entendamos o problema: o número 111...11, com k 1's, nada mais é que

$$\frac{10^k - 1}{9}.$$

O que queremos, então, é mostrar que, se n não é divisível nem por 2, nem por 5, existe um inteiro positivo k tal que $\frac{10^k - 1}{9}$ é divisível por n.

Ora, se n não é divisível nem por 2, nem por 5, $\text{mdc}(n, 10) = 1$. Mais que isso, na verdade, $\text{mdc}(9n, 10) = 1$ (9 também não tem nenhum fator em comum com 10). Daí, o teorema de Euler nos diz que

$$10^{\phi(9n)} \equiv 1 \pmod{9n},$$

ou seja,

$$9n \mid 10^{\phi(9n)} - 1.$$

[1] Verifique!

Isso quer dizer que existe um inteiro m tal que

$$10^{\phi(9n)} - 1 = 9n \cdot m.$$

Como essa igualdade é equivalente a

$$\frac{10^{\phi(9n)} - 1}{9} = n \cdot m,$$

concluímos que

$$n \mid \frac{10^{\phi(9n)} - 1}{9}.$$

4. Queremos mostrar que existem infinitos números da forma $10^k + 9(10^{k-1} + 10^{k-2} + \cdots + 10^2 + 10) + 1$ que são divisíveis por 1991. Observe, antes de mais nada, que

$$10^{k-1} + 10^{k-2} + \cdots + 10^2 + 10 = \frac{10^k - 10}{9}.$$

Assim, o que queremos é mostrar que existem infinitos $k \in \mathbb{N}$ para os quais $10^k + 10^k - 10 + 1 = 2 \cdot 10^k - 9$ é divisível por 1991. Veja agora que

$$2 \cdot 10^k - 9 \equiv 0 \pmod{1991} \iff 2 \cdot 10^k - 9 \equiv 1991 \pmod{1991} \iff 2 \cdot 10^k \equiv 2000 \pmod{1991}.$$

Como $\text{mdc}(1991, 2) = 1$, segue que a congruência é equivalente a

$$10^k \equiv 1000 \pmod{1991}.$$

Por fim, como $\text{mdc}(1991, 10) = 1$, esta última equivale a

$$10^{k-3} \equiv 1 \pmod{1991}.$$

Portanto, o problema se resume a demonstrar que existem infinitos $k \in \mathbb{N}$ tais que

$$10^{k-3} \equiv 1 \pmod{1991}.$$

Como $\text{mdc}(10, 1991) = 1$, segue do Teorema de Euler que $10^{\phi(1991)} \equiv 1 \pmod{1991}$. Daí, se $k = \phi(1991) \cdot m + 3$ para algum $m \in \mathbb{N}$, temos

$$10^{k-3} \equiv 10^{\phi(1991) \cdot m} \equiv (10^{\phi(1991)})^m \equiv 1^m \equiv 1 \pmod{1991}.$$

Como existem infinitos números da forma $\phi(1991) \cdot m + 3$ (um para cada valor de m), concluímos que existem infinitos $k \in \mathbb{N}$ para os quais $10^{k-3} \equiv 1 \pmod{1991}$.

Dessa forma, existem infinitos números da forma 1999...91 que são divisíveis por 1991.

5. O truque é utilizar que $\text{mdc}(a, n) = \text{mdc}(n - a, n)$. Com isso, concluímos que $\text{mdc}(a, n) = 1 \iff \text{mdc}(n - a, n) = 1$. Além disso, é claro também que $0 < a < n \iff 0 < (n - a) < n$. Daí,

$$\sum_{\substack{0 < a < n \\ \text{mdc}(a,n)=1}} a = \sum_{\substack{0 < a < n \\ \text{mdc}(a,n)=1}} (n - a),$$

pois em ambos os somatórios somamos cada inteiro entre 0 e n que é primo relativo com n exatamente uma vez. Dessa forma,

$$\begin{aligned} 2 \cdot \sum_{\substack{0<a<n \\ \text{mdc}(a,n)=1}} a &= \sum_{\substack{0<a<n \\ \text{mdc}(a,n)=1}} a + \sum_{\substack{0<a<n \\ \text{mdc}(a,n)=1}} (n-a) \\ &= \sum_{\substack{0<a<n \\ \text{mdc}(a,n)=1}} [a + (n-a)] \\ &= \sum_{\substack{0<a<n \\ \text{mdc}(a,n)=1}} n = n\phi(n). \end{aligned}$$

Portanto,

$$\sum_{\substack{0<a<n \\ \text{mdc}(a,n)=1}} a = \frac{n\phi(n)}{2}.$$

Esse resultado pode ser interpretado como uma demonstração de que a média dos $\phi(n)$ inteiros entre 0 e n que são primos com n (ou seja, cujo mdc com n é igual a 1) é sempre igual a $\frac{n}{2}$. E isso acontece porque, como vimos, a é um tal número se, e somente se, $n - a$ também o é.

6. Como $\text{mdc}(m, n) = 1$, segue do Teorema de Euler que $m^{\phi(n)} \equiv 1 \pmod{n}$. Além disso, $n^{\phi(m)} \equiv 0 \pmod{n}$, já que $\phi(m) > 0$. Assim,

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{n},$$

ou seja,

$$n \mid m^{\phi(n)} + n^{\phi(m)} - 1.$$

Reciprocamente, vem do Teorema de Euler que $n^{\phi(m)} \equiv 1 \pmod{m}$. Como $\phi(n) > 0$, também temos que $m^{\phi(n)} \equiv 0 \pmod{m}$. Daí,

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{m},$$

ou seja,

$$m \mid m^{\phi(n)} + n^{\phi(m)} - 1.$$

Esses dois resultados, juntamente com o fato de que $\text{mdc}(m, n) = 1$, implicam

$$mn \mid m^{\phi(n)} + n^{\phi(m)} - 1,$$

ou seja,

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

7. Como $n + 1$ é primo e $n > 1$, n deve ser par. Além disso, n deve ser múltiplo de 3. De fato:

- se $n \equiv 1 \pmod{3}$, $n - 1 \equiv 0 \pmod{3}$, o que é um absurdo, porque $n > 4$, e $n - 1$ é primo;
- se $n \equiv 2 \pmod{3}$, $n + 1 \equiv 0 \pmod{3}$, o que é um absurdo, porque $n > 4$, e $n + 1$ é primo.

Dessa forma, $n = 2^\alpha \cdot 3^\beta \cdot m$, para alguns $\alpha \geq 1$, $\beta \geq 1$ e m inteiros, com $\text{mdc}(m, 6) = 1$. Daí,

$$\phi(n) = 2^{\alpha-1} \cdot 2 \cdot 3^{\beta-1} \cdot \phi(m) = 2^\alpha \cdot 3^{\beta-1} \cdot \phi(m) \leq \frac{2^\alpha \cdot 3^\beta \cdot \phi(m)}{3}.$$

Como $\phi(m) \leq m$ (a igualdade ocorre quando $m = 1$), segue que

$$\phi(n) \leq \frac{2^\alpha \cdot 3^\beta \cdot m}{3} = \frac{n}{3}.$$

8. Vamos contar a quantidade de números no conjunto $\{1, 2, \ldots, n\}$. Por um lado, é claro que essa quantidade é igual a n. Por outro lado...

Se $a \in \{1, 2, \ldots, n\}$ é um número qualquer, $a = \text{mdc}(a,\, n) \cdot k$ para algum inteiro $1 \leq k \leq \frac{n}{\text{mdc}(a,\, n)}$ tal que $\text{mdc}\left(k,\, \frac{n}{\text{mdc}(a,\, n)}\right) = 1$. Por definição, $\text{mdc}(a,\, n)$ é um divisor de n.

Reciprocamente, se escolhemos um divisor d de n e um inteiro $1 \leq k \leq \frac{n}{d}$ tal que $\text{mdc}(k,\, \frac{n}{d}) = 1$, o número $d \cdot k$ será um inteiro entre 1 e n cujo mdc com n é igual a d.

Portanto, a quantidade de números no conjunto $\{1, 2, \ldots, n\}$ é exatamente igual à quantidade de pares $(d,\, k)$ em que d é um divisor de n e k é um inteiro entre 1 e $\frac{n}{d}$ tal que $\text{mdc}(k,\, \frac{n}{d}) = 1$. Para cada d, existem exatamente $\phi\left(\frac{n}{d}\right)$ inteiros k entre 1 e $\frac{n}{d}$ tais que $\text{mdc}(k,\, \frac{n}{d}) = 1$. Dessa forma, a quantidade de números no conjunto $\{1, 2, \ldots, n\}$ é igual a

$$\sum_{d\,|\,n} \phi\Big(\frac{n}{d}\Big).$$

De onde saiu a fórmula do enunciado? Ora, no somatório acima, estamos somando nada mais, nada menos, que o ϕ de todos os divisores de n. De fato, quando d varia entre os divisores de n, $\frac{n}{d}$ também varia entre os divisores de n. Então,

$$\sum_{d\,|\,n} \phi\Big(\frac{n}{d}\Big) = \sum_{d\,|\,n} \phi(d).$$

Portanto,

$$\sum_{d\,|\,n} \phi(d) = n.$$

9. Como $\text{mdc}(2,\, 5^{2000}) = 1$, segue do Teorema de Euler que $2^{\phi(5^{2000})} \equiv 1 \pmod{5^{2000}}$. Assim, existe $k \in \mathbb{N}$ tal que

$$2^{\phi(5^{2000})} = 5^{2000} \cdot k + 1.$$

Daí,

$$2^{2000+\phi(5^{2000})} = 2^{2000} \cdot 5^{2000} \cdot k + 2^{2000} = 10^{2000} \cdot k + 2^{2000}.$$

Assim,

$$2^{2000+\phi(5^{2000})} \;\equiv\; 2^{2000} \pmod{10^{2000}},$$

ou seja, os últimos 2000 algarismos de $2^{2000+\phi(5^{2000})}$ coincidem com os últimos 2000 algarismos de 2^{2000}. Mas

$$2^{2000} \;<\; (2^3)^{667} \;=\; 8^{667} \;<\; 10^{667},$$

ou seja, 2^{2000} tem menos de 668 algarismos.

Dessa forma, dentre os últimos 2000 algarismos de $2^{2000+\phi(5^{2000})}$ há ao menos 1033 zeros consecutivos.

10. Seja k um número natural qualquer.

Se $k = 0$, qualquer n serve.

Se $k = 1$, podemos tomar $n = 1$.

Suponhamos, então, $k > 1$.

Seja p o menor primo que não divide k.

Escrevamos

$$p - 1 = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_m^{\alpha_m},$$

a fatoração em primos de $p-1$. Pela definição de p, cada um dos primos q_i divide k. Podemos escrever, então,

$$k = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_m^{\beta_m} \cdot k',$$

para alguns $\beta_1, \beta_2, \ldots, \beta_m$, todos maiores que 0, e algum inteiro k', que não é divisível por nenhum dos q_i.

Seja $n := (p-1)k$.

Nesse contexto, temos

$$\phi(n+k) \;=\; \phi(pk) \;=\; \phi(p)\phi(k) \;=\; (p-1)\phi(k),$$

já que $\text{mdc}(p,\, k) = 1$ (pois p é primo e não divide k), e

$$\begin{aligned}
\phi(n) \;&=\; \phi\big((p-1)k\big) \;=\; \phi\big(q_1^{\alpha_1+\beta_1} \cdot q_2^{\alpha_2+\beta_2} \cdots q_m^{\alpha_m+\beta_m} \cdot k'\big) \\
&=\; (q_1-1)q_1^{\alpha_1+\beta_1-1} \cdot (q_2-1)q_2^{\alpha_2+\beta_2-1} \cdots (q_m-1)q_m^{\alpha_m+\beta_m-1} \cdot \phi(k') \\
&=\; \big(q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_m^{\alpha_m}\big)\big((q_1-1)q_1^{\beta_1-1} \cdot (q_2-1)q_2^{\beta_2-1} \cdots (q_m-1)q_m^{\beta_m-1} \cdot \phi(k')\big) \\
&=\; (p-1)\phi(k).
\end{aligned}$$

Logo, $\phi(n+k) = \phi(n)$.

11. Para facilitar a escrita, chamemos os i-ésimo termo da sequência de a_i.

Procederemos por indução.

Se $n = 2$, todos os termos da sequência são divisíveis por n e, portanto, são congruentes ao mesmo resto 0 módulo n.

Suponhamos que a afirmação seja válida para todo $n < n_0$, isto é, que para cada $n < n_0$, existe um índice k_n tal que $a_i \equiv a_j \pmod{n} \quad \forall \;\; i, j \geq k_n$. Vamos mostrar que existe k_{n_0} tal que $a_i \equiv a_j \pmod{n_0} \quad \forall \;\; i, j \geq k_{n_0}$.

Se n_0 é par, $n_0 = 2^\alpha \cdot m$ com m ímpar, podemos tomar $k_{n_0} = \max\{\alpha,\, k_m\}$. De fato, $a_i \equiv 0 \pmod{2^\alpha} \quad \forall \;\; i \geq \alpha$, e $a_i \equiv a_j \pmod{m} \quad \forall \;\; i, j \geq k_m$, de modo que $a_i \equiv a_j \pmod{2^\alpha \cdot m} \quad \forall \;\; i, j \geq \max\{\alpha, k_m\}$ (teorema Chinês dos Restos).

Suponhamos, então, que n_0 seja ímpar. Pelo teorema de Euler, $2^{\phi(n_0)} \equiv 1 \pmod{n_0}$. Isso implica que, se $a \equiv b \pmod{\phi(n_0)}$, então $2^a \equiv 2^b \pmod{n_0}$. De fato, se $a \equiv b \pmod{\phi(n_0)}$, existe $t \in \mathbb{Z}$ tal que $a = \phi(n_0) \cdot t + b$ e, então, $2^a \equiv (2^{\phi(n_0)})^t \cdot 2^b \equiv 2^b \pmod{n_0}$.

Pela hipótese de indução, existe $k \in \mathbb{N}$ tal que $a_i \equiv a_j \pmod{\phi(n_0)} \quad \forall \;\; i, j \geq k$. Daí, se $i, j \geq k+1$,

$$a_i \;\equiv\; 2^{a_{i-1}} \;\equiv\; 2^{a_{j-1}} \;\equiv\; a_j \pmod{n_0}.$$

Portanto, nesse caso, podemos fazer $k_{n_0} = k + 1$.

12. Se m é um natural ímpar,

$$\phi(2m) = \phi(m).$$

Com vista nisso, mostraremos que

$$\phi(n) \geq \sqrt{2n}$$

para todo n ímpar distinto de 3.

Se m e n são primos entre si e tais que

$$\phi(m) \;\geq\; \sqrt{2m} \quad \text{e} \quad \phi(n) \;\geq\; \sqrt{2n},$$

então

$$\phi(mn) \;=\; \phi(m)\phi(n) \;\geq\; \sqrt{4mn} \;>\; \sqrt{2mn}. \tag{1}$$

Dessa forma, é suficiente que provemos o resultado para as potências de primos.

Comecemos pelas potências de 3: seja 3^α uma potência de 3 com $\alpha > 1$. Temos

$$\phi(3^\alpha) \;=\; 2 \cdot 3^{\alpha-1} \;=\; 6 \cdot 3^{\alpha-2} \;>\; \sqrt{18} \cdot 3^{\alpha-2} \;\geq\; \sqrt{18 \cdot 3^{\alpha-2}} \;=\; \sqrt{2 \cdot 3^\alpha}.$$

Agora, seja p^α uma potência de um primo ímpar distinto de 3 (desta vez, α pode ser qualquer inteiro positivo, inclusive 1). Temos

$$\phi(p^\alpha) \;=\; (p-1) \cdot p^{\alpha-1} \;>\; \sqrt{2p} \cdot p^{\alpha-1} \;\geq\; \sqrt{2p \cdot p^{\alpha-1}} \;=\; \sqrt{2p^\alpha},$$

sendo a primeira desigualdade válida porque

$$p \geq 5 \;\Rightarrow\; p^2 > 4p - 1 \;\Rightarrow\; p^2 - 2p + 1 > 2p \;\Rightarrow\; (p-1)^2 > 2p \;\Rightarrow\; (p-1) > \sqrt{2p}.$$

Assim, $\phi(n) \geq \sqrt{2n}$ sempre que n for distinto de 3 e igual a uma potência de um primo ímpar. Daí, por (1),

$$\phi(n) \;\geq\; \sqrt{2n} \quad \text{para todo } n \text{ ímpar maior que 3.}$$

Com isso, já conseguimos provar a desigualdade do enunciado para os inteiros da forma $2^\alpha \cdot m$, com m ímpar e maior que 3: temos

$$\phi(2^\alpha \cdot m) \;=\; 2^{\alpha-1} \cdot \phi(m) \;\geq\; 2^{\alpha-1}\sqrt{2m} \;\geq\; \sqrt{2^{\alpha-1} \cdot 2m} \;=\; \sqrt{2^\alpha \cdot m}.$$

Olhemos agora para as potências de 2: se 2^α é uma potência de 2 com $\alpha > 1$,

$$\phi(2^\alpha) \;=\; 2^{\alpha-1} \;=\; 2 \cdot 2^{\alpha-2} \;=\; \sqrt{4} \cdot 2^{\alpha-1} \;\geq\; \sqrt{4 \cdot 2^{\alpha-2}} \;=\; \sqrt{2^\alpha}.$$

Restam somente os números da forma $2^\alpha \cdot 3$ com $\alpha > 1$, e o número 3. Para o 3 é fácil:

$$\phi(3) \;=\; 2 \;=\; \sqrt{4} \;>\; \sqrt{3}.$$

Por fim, se $2^\alpha \cdot 3$ é tal que $\alpha > 1$, então

$$\phi(2^\alpha \cdot 3) \;=\; 2^\alpha \;=\; 4 \cdot 2^{\alpha-2} \;>\; \sqrt{12} \cdot 2^{\alpha-2} \;\geq\; \sqrt{12 \cdot 2^{\alpha-2}} \;=\; \sqrt{2^\alpha \cdot 3}.$$

13. Seja $1 \leq i \leq 1000$.

- Se i é par, é claro que não existe inteiro j tal que $i \mid 2^j - 1$.
- Se i é ímpar, o teorema de Euler nos garante que $i \mid 2^{\phi(i)} - 1$. Como $1 \leq i \leq 1000$, $1 \leq \phi(i) \leq 1000$.

Dessa forma, existe $1 \leq j \leq 1000$ tal que $i \mid 2^j - 1$ se, e somente se, i é ímpar.

Portanto, existem exatamente 500 inteiros $1 \leq i \leq 1000$ para os quais existe um inteiro $1 \leq j \leq 1000$ tal que $i \mid 2^j - 1$.

14. Queremos mostrar que existem infinitos números da forma $2 \cdot 10^k + 21$ que são divisíveis por 2021. Em outras palavras, queremos mostrar que existem infinitos inteiros positivos k tais que

$$2 \cdot 10^k + 21 \;\equiv\; 0 \pmod{2021}.$$

Veja que

$$\begin{aligned} 2 \cdot 10^k + 21 \equiv 0 \pmod{2021} &\iff 2 \cdot 10^k + 21 \equiv 2021 \pmod{2021} \\ &\iff 2 \cdot 10^k \equiv 2000 \pmod{2021} \\ &\iff 10^k \equiv 1000 \pmod{2021} \\ &\iff 10^{k-3} \equiv 1 \pmod{2021}, \end{aligned}$$

sendo a terceira equivalência válida porque $\text{mdc}(2, 2021) = 1$, e a quarta, porque $\text{mdc}(10, 2021) = 1$.

Como $\text{mdc}(10, 2021) = 1$, o teorema de Euler garante que $10^{\phi(2021)} \equiv 1 \pmod{2021}$. Daí, se $k = \phi(2021) \cdot m + 3$ para algum $m \in \mathbb{N}$,

$$10^{k-3} \equiv 10^{\phi(2021) \cdot m} \equiv (10^{\phi(2021)})^m \equiv 1^m \equiv 1 \pmod{2021}.$$

Logo, para que tenhamos $10^{k-3} \equiv 1 \pmod{2021}$, é suficiente que façamos $k = \phi(2021) \cdot m + 3$, para algum $m \in \mathbb{N}$. Como existem infinitos números dessa forma, existem infinitos k que respeitam a condição que buscamos satisfazer.

Portanto, existem infinitos números da forma 2000...021 que são divisíveis por 2021.