POTI
POLOS OLÍMPICOS DE TREINAMENTO INTENSIVO

Problemas Resolvidos

Nível 2

Congruências II

Material elaborado por Valentino Amadeus Sichinel

Problemas

1 Pequeno Teorema de Fermat

Problema 1. Encontre o resto da divisão de:

(a) 3^{31} por 7.
(b) 2^{1000} por 13.
(c) 128^{129} por 17.

Problema 2. Sejam p e q dois primos distintos e a um inteiro positivo tal que $a^q \equiv a \pmod{p}$ e $a^p \equiv a \pmod{q}$. Prove que $a^{pq} \equiv a \pmod{pq}$.

Problema 3. Mostre que existem infinitos números da forma 1000...01 que são divisíveis por 101.

Dica: 101 *é primo.*

Problema 4. Mostre que não existe inteiro positivo x tal que $103 \mid x^3 - 2$.

Dica: 103 *é primo.*

Problema 5. Sejam a e b inteiros positivos. Prove que $a^{12} \equiv b^{12} \pmod{91}$ se, e somente se, $\text{mdc}(a, 91) = \text{mdc}(b, 91)$.

Problema 6. Seja p um primo ímpar para o qual existe $x \in \mathbb{Z}$ tal que $x^2 \equiv -1 \pmod{p}$. Prove que $p \equiv 1 \pmod{4}$.

Problema 7. Encontre um inteiro positivo k tal que $5^k \equiv 97 \pmod{101}$.

Dica: 101 *é primo.*

Problema 8. Quantos números primos p existem tais que $27^p + 1$ é um múltiplo de p?

Problema 9. Um número da forma p^n, em que p é um número primo e n é um inteiro positivo, é dito *legal* se $p^n \mid 7^{p^n} + 1$. Determine a soma de todos os números legais.

Problema 10. Se um "googolplex" é $10^{10^{100}}$, que dia da semana será daqui a um googolplex de dias?

Obs.: Suponha que hoje seja um domingo.

Problema 11. Mostre que não existe inteiro positivo $n > 1$ tal que $n \mid 2^n - 1$.

Problema 12 (IMO)**.** Determine todos os inteiros positivos m tais que

$$\text{mdc}(m,\ 2^n + 3^n + 6^n - 1) = 1 \quad \forall\ n \in \mathbb{N}.$$

Dica: $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$.

2 Teorema de Wilson

Problema 13. Seja n um número natural. Calcule $\text{mdc}\left(n! + 1,\ (n+1)!\right)$.

Problema 14. Seja p um primo ímpar. Mostre que

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Problema 15. Seja p um número primo tal que $p \equiv 1 \pmod{4}$. Prove que a congruência $x^2 \equiv -1 \pmod{p}$ tem solução.

Obs.: Compare este resultado com o do problema 6.

Problema 16 (IMO)**.** Determine todos os inteiros positivos n para os quais o conjunto

$$\{n,\ n+1,\ n+2,\ n+3,\ n+4,\ n+5\}$$

pode ser repartido em dois subconjuntos de tal maneira que o produto dos elementos de um é igual ao produto dos elementos do outro.

Soluções

1. (a) 7 é primo e não divide 3. Assim, pelo Pequeno Teorema de Fermat, $3^6 \equiv 1 \pmod 7$. Logo,

$$3^{31} \equiv 3^{30} \cdot 3 \equiv (3^6)^5 \cdot 3 \equiv 1^5 \cdot 3 \equiv 3 \pmod 7.$$

(b) 13 é primo e não divide 2. Assim, pelo Pequeno Teorema de Fermat, $2^{12} \equiv 1 \pmod{13}$. Logo,

$$2^{1000} \equiv 2^{996} \cdot 2^4 \equiv (2^{12})^{83} \cdot 2^4 \equiv 1^{83} \cdot 2^4 \equiv 2^4 \equiv 16 \equiv 3 \pmod{13}.$$

(c) 17 é primo e não divide 128. Assim, pelo Pequeno Teorema de Fermat, $128^{16} \equiv 1 \pmod{17}$. Logo,

$$128^{129} \equiv 128^{128} \cdot 128 \equiv (128^{16})^8 \cdot 128 \equiv 1^8 \cdot 128 \equiv 128 \equiv 9 \pmod{17}.$$

2. Pelo Pequeno Teorema de Fermat, $a^p \equiv a \pmod p$. Assim,

$$a^{pq} \equiv (a^p)^q \equiv a^q \equiv a \pmod p.$$

Da mesma forma, o Pequeno Teorema de Fermat nos conta que $a^q \equiv a \pmod q$, o que implica

$$a^{pq} \equiv (a^p)^q \equiv a^q \equiv a \pmod q.$$

Assim, temos que $p \mid (a^{pq} - a)$ e $q \mid (a^{pq} - a)$. Como p e q são primos distintos, isso implica $pq \mid (a^{pq} - a)$. Portanto, $a^{pq} - a \equiv 0 \pmod{pq}$, ou seja, $a^{pq} \equiv a \pmod{pq}$.

3. Queremos mostrar que existem infinitos números da forma $10^k + 1$ que são divisíveis por 101. Observe que

$$10^k + 1 \equiv 0 \pmod{101} \iff 10^k \equiv 100 \pmod{101} \iff 10^{k-2} \equiv 1 \pmod{101}.$$

Como 101 é primo e $101 \nmid 10$, sabemos, pelo Pequeno Teorema de Fermat, que $10^{100} \equiv 1 \pmod{101}$. Assim, se $k - 2 = 100 \cdot t$ para algum t (inteiro positivo), temos

$$10^{k-2} \equiv 10^{100t} \equiv (10^{100})^t \equiv 1^t \equiv 1 \pmod{101}.$$

Dessa forma, para que $10^k + 1$ seja múltiplo de 101, é suficiente que tenhamos $k - 2 = 100 \cdot t$ para algum t inteiro positivo, isto é, é suficiente que tenhamos $k = 100t + 2$, para algum t inteiro positivo. Como existem infinitos números da forma $100t + 2$, concluímos que existem infinitos números da forma $10^k + 1$ que são divisíveis por 101, isto é, que existem infinitos números da forma 1000...01 que são divisíveis por 101.

4. Suponhamos, por absurdo, que existe $x \in \mathbb{Z}$ tal que $103 \mid x^3 - 2$, isto é, tal que

$$x^3 - 2 \equiv 0 \pmod{103} \iff x^3 \equiv 2 \pmod{103}.$$

Como $2 \not\equiv 0 \pmod{103}$, $x^3 \not\equiv 0 \pmod{103}$. Como 103 é primo, isso é o mesmo que $x \not\equiv 0 \pmod{103}$. Sendo assim, segue do Pequeno Teorema de Fermat que $x^{102} \equiv 1 \pmod{103}$. Temos, então,

$$2^{34} \equiv (x^3)^{34} \equiv x^{102} \equiv 1 \pmod{103}.$$

Mas $2^{34} \not\equiv 1 \pmod{103}$. De fato,

$$2^{34} \equiv 2^{27} \cdot 2^7 \equiv (2^9)^3 \cdot 2^7 \equiv (512)^3 \cdot 128 \equiv (-3)^3 \cdot 25 \equiv -675 \equiv 46 \pmod{103}.$$

Dessa forma, nossa hipótese não se verifica, isto é, não há como existir $x \in \mathbb{Z}$ tal que $103 \mid x^3 - 2$.

5. Comecemos por fatorar 91: temos $91 = 7 \cdot 13$. Assim, para um inteiro x qualquer, temos

$$\mathrm{mdc}(x,\,91) \;=\; \begin{cases} 91, & \text{se } 7 \mid x \;\text{ e }\; 13 \mid x \\ 13, & \text{se } 7 \nmid x \;\text{ e }\; 13 \mid x \\ 7, & \text{se } 7 \mid x \;\text{ e }\; 13 \nmid x \\ 1, & \text{se } 7 \nmid x \;\text{ e }\; 13 \nmid x \end{cases}. \tag{1}$$

Além disso, segue da fatoração que

$$x \equiv y \pmod{91} \iff \begin{cases} x \equiv y \pmod{7} \\ x \equiv y \pmod{13} \end{cases}, \tag{2}$$

sejam quais forem os inteiros x e y.

7 é primo. Logo, pelo Pequeno Teorema de Fermat,

$$7 \nmid x \iff x^6 \equiv 1 \pmod{7} \Rightarrow x^{12} \equiv 1 \pmod{7}.$$

Como $x^{12} \equiv 1 \pmod{7}$ implica $7 \nmid x$, temos, na verdade, a equivalência

$$7 \nmid x \iff x^{12} \equiv 1 \pmod{7}.$$

Daí, vem que

$$x^{12} \equiv \begin{cases} 0 \pmod{7}, & \text{se } 7 \mid x \\ 1 \pmod{7}, & \text{se } 7 \nmid x \end{cases}. \tag{3}$$

Por fim, 13 é primo, donde, pelo Pequeno Teorema de Fermat,

$$13 \nmid x \;\Rightarrow\; x^{12} \equiv 1 \pmod{13},$$

seja qual for $x \in \mathbb{Z}$. Disso, segue que

$$x^{12} \equiv \begin{cases} 0 \pmod{13}, & \text{se } 13 \mid x \\ 1 \pmod{13}, & \text{se } 13 \nmid x \end{cases}, \tag{4}$$

para todo $x \in \mathbb{Z}$.

Agora, é só juntar as informações.

Por (1), (3) e (4), temos

$$\mathrm{mdc}(x,\,91) \;=\; \begin{cases} 91, & \text{se } x^{12} \equiv 0 \pmod{7} \;\text{ e }\; x^{12} \equiv 0 \pmod{13} \\ 13, & \text{se } x^{12} \equiv 1 \pmod{7} \;\text{ e }\; x^{12} \equiv 0 \pmod{13} \\ 7, & \text{se } x^{12} \equiv 0 \pmod{7} \;\text{ e }\; x^{12} \equiv 1 \pmod{13} \\ 1, & \text{se } x^{12} \equiv 1 \pmod{7} \;\text{ e }\; x^{12} \equiv 1 \pmod{13} \end{cases}.$$

Isso mostra que, para inteiros x e y,

$$\mathrm{mdc}(x,\,91) = \mathrm{mdc}(y,\,91) \iff \begin{cases} x^{12} \equiv y^{12} \pmod{7} \\ x^{12} \equiv y^{12} \pmod{13} \end{cases}.$$

Aplicando esta última equivalência, juntamente com a equivalência (2), aos inteiros a e b, concluímos que

$$a^{12} \equiv b^{12} \pmod{91} \iff \mathrm{mdc}(a,\,91) = \mathrm{mdc}(b,\,91),$$

tal como queríamos.

6. Se $x^2 \equiv -1 \pmod{p}$, $p \nmid x$. Assim, pelo Pequeno Teorema de Fermat, $x^{p-1} \equiv 1 \pmod{p}$. Como p é ímpar, $\frac{p-1}{2}$ é inteiro. Daí,

$$\begin{aligned} x^2 \equiv -1 \pmod{p} &\Rightarrow x^{p-1} \equiv (-1)^{(p-1)/2} \pmod{p} \\ &\Rightarrow (-1)^{(p-1)/2} \equiv 1 \pmod{p} \Rightarrow \frac{p-1}{2} \equiv 0 \pmod{2} \\ &\Rightarrow p \equiv 1 \pmod{4}. \end{aligned}$$

7. Observe que $97 \equiv -4 \pmod{101}$. Assim, queremos encontrar k tal que $5^k \equiv -4 \pmod{101}$. Como $\text{mdc}(101, 25) = 1$, essa congruência é equivalente a $5^{k+2} \equiv -100 \pmod{101}$. E $-100 \equiv 1 \pmod{101}$. Dessa forma, o que queremos é encontrar k tal que $5^{k+2} \equiv 1 \pmod{101}$.

Como 101 é primo e $101 \nmid 5$, segue do Pequeno Teorema de Fermat que $5^{100} \equiv 1 \pmod{101}$. Portanto, para alcançar nosso objetivo, podemos fazer $k = 98$.

8. É claro que se $27^p + 1$ é múltiplo de p, p não divide 27. Assim, se p é um número primo tal que $27^p + 1 \equiv 0 \pmod{p}$, temos, pelo Pequeno Teorema de Fermat, que $27^p \equiv 27 \pmod{p}$.

Combinando as duas congruências, ficamos com $28 \equiv 27 + 1 \equiv 27^p + 1 \equiv 0 \pmod{p}$, isto é, p deve dividir 28. Os únicos primos que dividem 28 são 2 e 7.

Será que 2 e 7 satisfazem a condição do enunciado? A resposta é sim, e para verificar, basta percorrer o caminho inverso: se $p = 2$ ou 7,

$$27^p + 1 \equiv 27 + 1 \equiv 28 \equiv 0 \pmod{p}.$$

Portanto, há exatamente dois números primos p tais que $27^p + 1$ é um múltiplo de p.

9. Sejam p um número primo e n um inteiro positivo tais que p^n é um número legal.

De $p^n \mid 7^{p^n} + 1$, segue que $p \nmid 7$. Daí, pelo Pequeno Teorema de Fermat, $7^{p-1} \equiv 1 \pmod{p}$. Além disso, $p^n \equiv 1 \pmod{p-1}$ (já que $p \equiv 1 \pmod{p-1}$), donde existe $k \in \mathbb{N}$ tal que $p^n = (p-1)k + 1$. Assim,

$$7^{p^n} + 1 \equiv 7^{(p-1)k+1} + 1 \equiv (7^{p-1})^k \cdot 7 + 1 \equiv 1^k \cdot 7 + 1 \equiv 8 \pmod{p}.$$

Mas $p \mid 7^{p^n} + 1$, pois $p \mid p^n$ e $p^n \mid 7^{p^n} + 1$. Logo, $p \mid 8$, donde p deve ser igual a 2.

Como $7 \equiv -1 \pmod{4}$, $7^{2^n} \equiv 1 \pmod{4}$, seja qual for o inteiro $n \geq 1$. Assim, $7^{2^n} + 1 \equiv 2 \pmod{4}$ $\forall\, n \geq 1$, donde $4 \nmid 7^{2^n} + 1$.

Dessa forma, para que 2^n seja legal, n deve ser no máximo 1. Em outras palavras, 2 é o único possível número legal. Como $2 \mid 7^2 + 1$, 2 é, de fato, legal.

Portanto, a soma de todos os números legais é igual a 2.

10. Como os dias da semana se repetem em um ciclo de tamanho 7, queremos saber qual o resto da divisão de um googolplex por 7.

Pelo Pequeno Teorema de Fermat, $10^6 \equiv 1 \pmod{7}$. Para utilizar isso a nosso favor na hora de calcular $10^{10^{100}} \pmod{7}$, precisamos decompor 10^{100} em um múltiplo de 6 e um resto.

Observe que $10^2 \equiv 100 \equiv 10 \pmod{6}$. Daí, $10^k \equiv 10^2 \cdot 10^{k-2} \equiv 10 \cdot 10^{k-2} \equiv 10^{k-1} \pmod{6}$ para todo $k \geq 2$ inteiro. Consequentemente,

$$10^{100} \equiv 10^{99} \equiv 10^{98} \equiv 10^{97} \equiv \ldots \equiv 10^3 \equiv 10^2 \equiv 10 \equiv 4 \pmod{6}.$$

Isso quer dizer que existe um inteiro k tal que $10^{100} = 6k + 4$.

Dessa forma,

$$10^{10^{100}} \equiv 10^{6k+4} \equiv (10^6)^k \cdot 10^4 \equiv 1^k \cdot 10^4 \equiv 10^4 \equiv 3^4 \equiv 81 \equiv 4 \pmod{7}.$$

Portanto, o dia da semana em que estaremos daqui a um googolplex de dias será 4 dias da semana depois do dia de hoje. Se hoje é domingo, então, daqui a um googolpex de dias será uma quinta-feira.

11. Suponhamos, por absurdo, que $n > 1$ seja um inteiro tal que $n \mid 2^n - 1$.

Seja p o menor fator primo de n. Como $n \mid 2^n - 1$, $p \mid 2^n - 1$. Daí, p deve ser distinto de 2. Pelo Pequeno Teorema de Fermat, então, $p \mid 2^{p-1} - 1$. De que maneira podemos combinar essas duas informações (a saber, a informação de que $p \mid 2^n - 1$ e a informação de que $p \mid 2^{p-1} - 1$)?

A resposta está no teorema de Bézout[1]. Como p é o menor fator primo de n, os fatores primos de $p - 1$ são menores que qualquer fator primo de n e, assim, $\text{mdc}(p - 1,\, n) = 1$ - eis o motivo pelo qual escolhemos p como sendo *o menor* fator primo de n. Dessa forma, existem inteiros a e b tais que $a(p - 1) + bn = 1$. Como $p - 1$ e n são ambos maiores que 1, ou a é positivo e b é negativo, ou a é negativo e b é positivo.

Se a é positivo e b é negativo, temos $a(p - 1) = |b|n + 1$. Daí,

$$1 \;\equiv\; 1^a \;\equiv\; (2^{p-1})^a \;\equiv\; 2^{a(p-1)} \;\equiv\; 2^{|b|n+1} \;\equiv\; (2^n)^{|b|} \cdot 2 \;\equiv\; 1^{|b|} \cdot 2 \;\equiv\; 2 \pmod{p}.$$

Absurdo!

Por outro lado, se a é negativo e b é positivo, temos $bn = |a|(p - 1) + 1$. Daí,

$$1 \;\equiv\; 1^b \;\equiv\; (2^n)^b \;\equiv\; 2^{nb} \;\equiv\; 2^{|a|(p-1)+1} \;\equiv\; (2^{p-1})^{|a|} \cdot 2 \;\equiv\; 1^{|a|} \cdot 2 \;\equiv\; 2 \pmod{p}.$$

Absurdo também!

Portanto, não é possível que haja $n \in \mathbb{N}$, $n > 1$, tal que $n \mid 2^n - 1$.

12. Afirmamos que nenhum inteiro positivo maior que 1 é primo com todos os termos da sequência $\{2^n + 3^n + 6^n - 1\}_{n\geq 1}$. Para vermos isso, é suficiente que provemos que cada primo divide ao menos um elemento da sequência.

Antes de mais nada, observemos que todos os termos da sequência são pares. Assim, 2 divide todos eles. Além disso, o segundo termo da sequência é divisível por 3. De fato, temos

$$2^2 + 3^2 + 6^2 - 1 \;\equiv\; 2^2 - 1 \;\equiv\; 3 \;\equiv\; 0 \pmod{3}.$$

Dessa forma, basta olharmos para os primos p diferentes de 2 e de 3.

Seja, então, p um primo distinto de 2 e de 3.

Como $p \nmid 2$, $p \nmid 3$ e $p \nmid 6$, o Pequeno Teorema de Fermat nos garante que

$$2^{p-1} \equiv 1 \pmod{p}, \qquad 3^{p-1} \equiv 1 \pmod{p} \quad \text{e} \quad 6^{p-1} \equiv 1 \pmod{p}.$$

Daí, segue que

$$6\big(2^{p-2} + 3^{p-2} + 6^{p-2}\big) \;\equiv\; 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} \;\equiv\; 3 + 2 + 1 \;\equiv\; 6 \pmod{p}.$$

Como $\text{mdc}(6,\, p) = 1$, isso implica

$$2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \pmod{p}.$$

Dessa forma, p divide $2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.

Como todos os primos dividem ao menos um termo da sequência $\{2^n + 3^n + 6^n - 1\}_{n\geq 1}$, não existe nenhum inteiro m maior que 1 tal que $\text{mdc}(m,\; 2^n + 3^n + 6^n - 1) = 1 \quad \forall \; n \in \mathbb{N}$. Portanto, o único inteiro positivo que satisfaz a condição expressa no enunciado é o número 1.

[1] O Teorema de Bézout diz que se x e y são inteiros tais que $\text{mdc}(x,\, y) = 1$, existem inteiros a e b tais que $ax + by = 1$.

13. Se p é um primo tal que $p \mid n!$, é claro que $p \nmid n!+1$. Por outro lado, se p é primo tal que $p \mid (n+1)!$, então $p \mid n!$ ou $p \mid (n+1)$. Dessa forma, para analisarmos os fatores primos de $\mathrm{mdc}\big(n!+1,\ (n+1)!\big)$, basta que olhemos para os fatores primos de $n+1$.

Se $n+1$ é composto, todos os seus fatores primos são estritamente menores que $n+1$ e, assim, dividem $n!$. Dessa forma, nesse caso, $\mathrm{mdc}\big(n!+1,\ (n+1)!\big) = 1$.

Por outro lado, se $n+1$ é primo, o teorema de Wilson nos diz que $n! \equiv -1 \pmod{n+1}$. Assim, nesse caso, $n+1 \mid n!+1$ e, então, $\mathrm{mdc}\big(n!+1,\ (n+1)!\big) = n+1$.

Portanto,

$$\mathrm{mdc}\big(n!+1,\ (n+1)!\big) = \begin{cases} 1, & \text{se } n+1 \text{ é composto} \\ n+1, & \text{se } n+1 \text{ é primo} \end{cases}.$$

14. Observe que

$$\begin{aligned}
(p-1)! &\equiv (p-1)\cdot(p-2)\cdots\Big(\frac{p+1}{2}\Big)\cdot\Big(\frac{p-1}{2}\Big)\cdots 2\cdot 1 \\
&\equiv (-1)\cdot(-2)\cdots\Big(-\big(\frac{p-1}{2}\big)\Big)\cdot\Big(\frac{p-1}{2}\Big)\cdots 2\cdot 1 \\
&\equiv (-1)^{(p-1)/2}\cdot 1^2\cdot 2^2\cdots\Big(\frac{p-1}{2}\Big)^2 \\
&\equiv (-1)^{(p-1)/2}\cdot\left(\Big(\frac{p-1}{2}\Big)!\right)^2 \pmod{p}.
\end{aligned}$$

Pelo Teorema de Wilson, $(p-1)! \equiv -1 \pmod{p}$. Assim,

$$(-1)^{(p-1)/2}\cdot\left(\Big(\frac{p-1}{2}\Big)!\right)^2 \pmod{p} \ \equiv\ -1 \pmod{p}$$

e, portanto,

$$\left(\Big(\frac{p-1}{2}\Big)!\right)^2 \ \equiv\ (-1)^{(p+1)/2} \pmod{p}.$$

15. Pelo problema anterior, se p é um primo tal que $p \equiv 1 \pmod 4$,

$$x := \Big(\frac{p-1}{2}\Big)!$$

é tal que $x^2 \equiv (-1)^{(p+1)/2} \equiv -1 \pmod{p}$.

16. Afirmamos que não há nenhum inteiro n que satisfaz a condição exposta no enunciado. Para vermos pro que, suponhamos por absurdo que n é tal que $\{n,\, n+1,\, n+2,\, n+3,\, n+4,\, n+5\}$ pode ser repartido em dois subconjuntos, A e B, o produto dos elementos de um sendo igual ao produto dos elementos do outro. Temos, então,

$$A \cap B = \emptyset, \qquad A \cup B = \{n,\, n+1,\, n+2,\, n+3,\, n+4,\, n+5\}$$

e

$$\prod_{a\in A} a = \prod_{b\in B} b.$$

Nenhum dos elementos de $\{n,\, n+1,\, n+2,\, n+3,\, n+4,\, n+5\}$ pode ser divisível por 7. De fato, como são seis inteiros consecutivos, se um deles fosse múltiplo de 7, nenhum outro seria, e então ou $\prod_{a\in A} a$ ou $\prod_{b\in B} b$ seria múltiplo de 7, mas não ambos (e isso nos conduziria a um absurdo, pois os produtos são iguais).

Dessa forma, como estamos lidando com seis inteiros consecutivos, nenhum dos quais divisível por 7,

$$n(n+1)(n+2)(n+3)(n+4)(n+5) \;\equiv\; 6! \pmod 7.$$

Pelo teorema de Wilson, $6! \equiv -1 \pmod 7$. Por outro lado,

$$n(n+1)(n+2)(n+3)(n+4)(n+5) = \left(\prod_{a\in A} a\right)\left(\prod_{b\in B} b\right) = \left(\prod_{a\in A} a\right)^2.$$

Assim,

$$\left(\prod_{a\in A} a\right)^2 \;\equiv\; -1 \pmod 7.$$

Isso é um absurdo, no entanto, conforme mostra o resultado do problema 6.