POTI
POLOS OLÍMPICOS DE TREINAMENTO INTENSIVO

Problemas Resolvidos

Nível 2

Congruências I

Material elaborado por Valentino Amadeus Sichinel

Problemas

Problema 1. Seja n um inteiro ímpar. Mostre que $n^2 - 1$ é divisível por 8.

Problema 2. Seja n um inteiro ímpar. Mostre que $n(n^2 - 1)$ é divisível por 24.

Problema 3. Seja n um inteiro ímpar que não é divisível por 3. Mostre que $n^2 - 1$ é divisível por 24.

Problema 4. Mostre que, se n é um inteiro ímpar, n^2 só pode deixar resto 1 ou 9 na divisão por 16.

Problema 5. Determine todos os restos possíveis da divisão de um cubo perfeito por 7.

Problema 6. Determine todos os restos possíveis da divisão de um cubo perfeito pro 9.

Problema 7. Sejam a e b números inteiros, e seja k um inteiro positivo qualquer. Mostre que $a - b$ divide $a^k - b^k$.

Problema 8. Sejam a e b números inteiros, e seja k um inteiro positivo ímpar. Mostre que $a + b$ divide $a^k + b^k$.

Problema 9. Seja n um inteiro positivo. Prove que $19^{8n} - 1$ é divisível por 17.

Problema 10. Prove que, se n é um inteiro positivo ímpar, então 45 divide $13^{3n} + 17^{3n}$.

Problema 11. Mostre que não existem inteiros x, y, z e w tais que $x^2 + y^2 + z^2 = 8w + 7$.

Problema 12. Mostre que todo número primo da forma $3k + 1$ é da forma $6n + 1$.

Problema 13. Mostre que não existem inteiros x e y tais que $x^3 - 117y^3 = 5$.

Problema 14 (IMO)**.** Mostre que a fração $\frac{21n+4}{14n+3}$ é irredutível para todo n natural.

Problema 15. Prove que, para todo inteiro positivo n,

(a) $n^3 - n$ é divisível por 3.
(b) $n^5 - n$ é divisível por 5.
(c) $n^7 - n$ é divisível por 7.

Obs.: Veja que $n^9 - n$ não é necessariamente divisível por 9*. De fato, $2^9 - 2 = 510$ não é divisível por 9.

Problema 16. Prove que $3^{6n} - 2^{6n}$ é divisível por 35, qualquer que seja o inteiro positivo n.

Problema 17. Seja $n > 2$ um número natural. Prove que se um dos números $2^n - 1$ e $2^n + 1$ é primo, então o outro é composto.

Problema 18. Prove que, se tanto p quanto $8p - 1$ são primos, então $8p + 1$ é composto.

Problema 19. Prove que, se tanto p quanto $8p^2 + 1$ são primos, então $8p^2 - 1$ também é primo.

Problema 20. Prove que $n^2 + 3n + 5$ nunca é divisível por 121, seja qual for o inteiro n.

*Os itens a-c são casos especiais de um teorema famoso. Para entender melhor, veja o material sobre o *pequeno teorema de Fermat*.

Soluções

1. Como n é ímpar, temos quatro possibilidades: podemos ter

$$n \equiv 1 \pmod 8, \quad \text{ou} \quad n \equiv 3 \pmod 8, \quad \text{ou} \quad n \equiv 5 \pmod 8, \quad \text{ou} \quad n \equiv 7 \pmod 8.$$

Analisemos cada caso separadamente.

- Se $n \equiv 1 \pmod 8$, $n^2 \equiv 1^2 \equiv 1 \pmod 8$, donde $n^2 - 1$ é divisível por 8.
- Se $n \equiv 3 \pmod 8$, $n^2 \equiv 3^2 \equiv 9 \equiv 1 \pmod 8$, donde $n^2 - 1$ é divisível por 8.
- Se $n \equiv 5 \pmod 8$, $n^2 \equiv 5^2 \equiv 25 \equiv 1 \pmod 8$, donde $n^2 - 1$ é divisível por 8.
- Se $n \equiv 7 \pmod 8$, $n^2 \equiv 7^2 \equiv 49 \equiv 1 \pmod 8$, donde $n^2 - 1$ é divisível por 8.

Dessa forma, se o inteiro n for ímpar, $n^2 - 1$ será divisível por 8, seja qual for o valor de n.

2. Como $\text{mdc}(8, 3) = 1$, para mostrarmos que $n(n^2 - 1)$ é divisível por $8 \times 3 = 24$, é suficiente que mostremos que $n(n^2 - 1)$ é divisível por 8 e por 3. Já vimos, no problema 1, que $n^2 - 1$ é divisível por 8. Basta mostrarmos, então, que $n(n^2 - 1)$ é divisível por 3. Temos três casos a analisar:

- se $n \equiv 0 \pmod 3$, $n(n^2 - 1) \equiv 0 \cdot (n^2 - 1) \equiv 0 \pmod 3$;
- se $n \equiv 1 \pmod 3$, $n(n^2 - 1) \equiv 1 \cdot (1^2 - 1) \equiv 1 \cdot 0 \equiv 0 \pmod 3$;
- se $n \equiv 2 \pmod 3$, $n(n^2 - 1) \equiv 2 \cdot (4 - 1) \equiv 2 \cdot 3 \equiv 0 \pmod 3$.

Em qualquer caso, $n(n^2 - 1)$ é divisível por 3. Como $n^2 - 1$ é divisível por 8, concluímos que $n(n^2 - 1)$ é divisível por $8 \times 3 = 24$.

3. Utilizaremos o resultado dos dois problemas anteriores.

Como n é ímpar, sabemos pelo problema 1 que $n^2 - 1$ é divisível por 8.

Além disso, vimos no problema 2 que $n(n^2 - 1)$ é divisível por 3. Isso quer dizer que ou 3 divide n, ou 3 divide $n^2 - 1$ (ou ambos). Bem, estamos supondo, neste problema, que n não é divisível por 3. Logo, $n^2 - 1$ há de ser divisível por 3.

Dessa forma, $n^2 - 1$ é divisível por 3 e por 8 e, portanto, por $3 \times 8 = 24$ (já que $\text{mdc}(3, 8) = 1$).

4. Vimos no problema 1 que, se n é ímpar, então n^2 deixa resto 1 na divisão por 8. Assim, sendo n ímpar, $n^2 = 8k + 1$, para algum inteiro k.

Se k é par, digamos, igual a $2k'$, $n^2 = 8k + 1 = 16k' + 1 \equiv 1 \pmod{16}$.

Se k é ímpar, digamos, igual a $2k' + 1$, $n^2 = 8k + 1 = 16k' + 8 + 1 \equiv 9 \pmod{16}$.

Portanto, dado que n é ímpar, n^2 só pode deixar resto 1 ou 9 quando dividido por 16.

5. Analisemos os casos.

- Se $n \equiv 0 \pmod 7$, $n^3 \equiv 0 \pmod 7$.
- Se $n \equiv 1 \pmod 7$, $n^3 \equiv 1 \pmod 7$.
- Se $n \equiv 2 \pmod 7$, $n^3 \equiv 8 \equiv 1 \pmod 7$.
- Se $n \equiv 3 \pmod 7$, $n^3 \equiv 27 \equiv -1 \pmod 7$.

Agora, utilizamos um pequeno truque, para encurtar os cálculos: seja qual for $n \in \mathbb{Z}$, $n^3 \equiv -(-n)^3 \pmod 7$. Bom, se n deixa um resto $r \geq 4$ quando dividido por 7, então $-n$ deixa um resto $7 - r \leq 3$ quando divido por 7. Assim, o resto de $(-n)^3$ (quando dividido por 7) é 0, 1 ou -1 e, portanto, o resto de n^3 quando divido por 7, que é o mesmo que o resto de $-(-n)^3$, só pode ser 0, -1 ou 1.

Dessa forma, se n é um número inteiro, então n^3 deixa resto 0, 1 ou -1 quando dividido por 7.

6. Analisemos os casos.

- Se $n \equiv 0 \pmod 9$, $n^3 \equiv 0 \pmod 9$.
- Se $n \equiv 1 \pmod 9$, $n^3 \equiv 1 \pmod 9$.
- Se $n \equiv 2 \pmod 9$, $n^3 \equiv 8 \equiv -1 \pmod 9$.
- Se $n \equiv 3 \pmod 9$, $n^3 \equiv 27 \equiv 0 \pmod 9$.
- Se $n \equiv 4 \pmod 9$, $n^3 \equiv 4 \cdot 16 \equiv 4 \cdot 7 \equiv 28 \equiv -1 \pmod 9$.

Agora, utilizamos um pequeno truque, para encurtar os cálculos: seja qual for $n \in \mathbb{Z}$, $n^3 \equiv -(-n)^3 \pmod 7$. Bom, se n deixa um resto $r \geq 5$ quando dividido por 9, então $-n$ deixa um resto $7 - r \leq 4$ quando divido por 9. Assim, o resto de $(-n)^3$ (quando dividido por 9) é 0, 1 ou -1 e, portanto, o resto de n^3 quando divido por 9, que é o mesmo que o resto de $-(-n)^3$, só pode ser 0, -1 ou 1.

Dessa forma, se n é um número inteiro, então n^3 deixa resto 0, 1 ou -1 quando dividido por 9.

Observação: O fato de haver apenas três possibilidades para o resto da divisão de um cubo perfeito por 9 pode ser útil em algumas situações. É um resultado que vale a pena ter em mente.

7. Observe que $a - b \equiv 0 \pmod{a-b} \iff a \equiv b \pmod{a-b}$.

Elevando à k-ésima potência, ficamos com $a^k \equiv b^k \pmod{a-b}$, isto é, $a^k - b^k \equiv 0 \pmod{a-b}$.

Dessa forma, $a - b$ divide $a^k - b^k$.

8. Observe que $a + b \equiv 0 \pmod{a+b} \iff a \equiv -b \pmod{a+b}$.

Elevando à k-ésima potência, ficamos com $a^k \equiv (-b)^k \equiv (-1)^k \cdot b^k \pmod{a+b}$. Como k é ímpar, $(-1)^k \cdot b^k \equiv (-1) \cdot b^k \equiv -b^k \pmod{a+b}$.

Logo, $a^k \equiv -b^k \pmod{a+b} \iff a^k + b^k \equiv 0 \pmod{a+b}$.

Dessa forma, $a + b$ divide $a^k + b^k$.

9. Temos $19 \equiv 2 \pmod{17}$. Logo, $19^{8n} - 1 \equiv 2^{8n} - 1 \pmod{17}$.

Observe agora que $2^4 \equiv 16 \equiv -1 \pmod{17}$. Dessa forma, $2^8 \equiv (2^4)^2 \equiv (-1)^2 \equiv 1 \pmod{17}$.

Assim, $2^{8n} \equiv (2^8)^n \equiv 1^n \equiv 1 \pmod{17}$.

Logo, $19^{8n} - 1 \equiv 2^{8n} - 1 \equiv 0 \pmod{17}$ e, portanto, 17 divide $19^{8n} - 1$.

10. Como $\text{mdc}(5, 9) = 1$ e $45 = 5 \times 9$, é suficiente analisarmos a divisibilidade por 5 e por 9 separadamente.

Em primeiro lugar, $13^{3n} + 17^{13} \equiv 3^{3n} + 2^{3n} \pmod 5$.

Como n é ímpar, $3n$ também o é. Pelo problema 8, isso implica que $2^{3n} + 3^{3n}$ é divisível por $2 + 3 = 5$.

Resta analisarmos, então, a divisibilidade por 9. Temos $13^{3n} + 17^{3n} \equiv 4^{3n} + (-1)^{3n} \pmod 9$.

Como $3n$ é ímpar, $(-1)^{3n} \equiv -1 \pmod 9$.

Além do mais, $4^2 \equiv 16 \equiv 7 \pmod 9$, donde $4^3 \equiv 4 \cdot 7 \equiv 28 \equiv 1 \pmod 9$ e, portanto, $4^{3n} \equiv (4^3)^n \equiv 1^n \equiv 1 \pmod 9$.

Assim, $13^{3n} + 17^{3n} \equiv 4^{3n} + (-1)^{3n} \equiv 1 - 1 \equiv 0 \pmod 9$.

Dessa forma, $13^{3n} + 17^{3n}$ é divisível tanto por 5 quanto por 9 e, portanto, por $5 \times 9 = 45$.

11. Queremos mostrar que não existem inteiros x, y e z tais que $x^2 + y^2 + z^2 \equiv 7 \pmod 8$. Analisemos, então, os possíveis restos de um quadrado módulo 8.

Se n é divisível por 4 (congruente a 0 ou a 4 módulo 8), n^2 é divisível por $4^2 = 16$. Em particular, n^2 é divisível por 8 e, portanto, é congruente a 0 módulo 8.

Se n é divisível por 2, mas não por 4, n é congruente a 2 ou a 6 módulo 8. Se $n \equiv 2 \pmod 8$, $n^2 \equiv 4 \pmod 8$. Se $n \equiv 6 \pmod 8$, $n^2 \equiv 36 \equiv 4 \pmod 8$.

Por fim, se n é ímpar, $n^2 \equiv 1 \pmod 8$ (de fato, pelo problema 1, $n^2 - 1$ é divisível por 8).

Portanto, os possíveis restos de um quadrado módulo 8 são 0, 1 e 4. Isto é: se n é um número inteiro, então ou $n^2 \equiv 0 \pmod 8$, ou $n^2 \equiv 1 \pmod 8$, ou $n^2 \equiv 4 \pmod 8$.

Suponhamos, agora, que x, y e z são três inteiros tais que $x^2 + y^2 + z^2 \equiv 7 \pmod 8$.

Se x, y e z fossem pares, $x^2 + y^2 + z^2$ também seria e, portanto, não poderia ser congruente a 7 módulo 8. Dessa forma, ao menos um dos inteiros é ímpar. Sem perder generalidade, suporemos que z é ímpar. Temos, então, $z^2 \equiv 1 \pmod 8$. Como $x^2 + y^2 + z^2 \equiv 7 \pmod 8$, isso implica $x^2 + y^2 \equiv 6 \pmod 8$.

Mas x^2 e y^2 só podem ser 0, 1 ou 4 módulo 8, de modo que $x^2 + y^2$ só pode ser 0, 1, 2, 4 ou 5 módulo 8. Absurdo!

Tendo nossa suposição nos levado a um absurdo, concluímos que não há maneira de ela ser válida. Em outras palavras: não existem inteiros x, y e z tais que $x^2 + y^2 + z^2 \equiv 7 \pmod 8$ (e, consequentemente, não existem inteiros x, y, z e w tais que $x^2 + y^2 + z^2 = 8w + 7$).

12. Suponhamos que $p = 3k + 1$ é um número primo.

Se $k \equiv 1 \pmod 2$, $3k + 1 \equiv 3 + 1 \equiv 4 \equiv 0 \pmod 2$. Logo, nesse caso, p é par. Como o único primo par é 2, $p = 2$. Mas 2 não é da forma $3k + 1$. Absurdo!

Dessa forma, devemos ter $k \equiv 0 \pmod 2$. Daí, existe um inteiro n tal que $k = 2n$. Temos então $p = 3k + 1 = 6n + 1$.

13. Suponhamos, por absurdo, que x e y são dois inteiros tais que $x^3 - 117y^3 = 5$. Essa igualdade nos indica, em particular, que $x^3 - 117y^3 \equiv 5 \pmod 9$. Bem, $117 \equiv 0 \pmod 9$. Logo, isso é o mesmo que $x^3 \equiv 5 \pmod 9$. No entanto, um cubo perfeito só pode deixar resto 0, 1 ou -1 quando dividido por 9. Absurdo! Dessa forma, não existem inteiros x e y tais que $x^3 - 117y^3 = 5$.

14. Entendamos, antes de mais nada, qual o nosso objetivo. Queremos mostrar que a fração é irredutível. Mas o que isso significa? Mostrar que uma fração é irredutível é o mesmo que mostrar que o numerador e o denominador não têm fator primo em comum. Por exemplo: a fração $\frac{5}{3}$ é irredutível, porque 5 e 3 não têm nenhum fator primo em comum. Por outro lado, a fração $\frac{10}{6}$ não é irredutível, já que tanto 10 quanto 6 são divisíveis por 2 (10 e 6 têm o fator primo 2 em comum).

O que devemos fazer, então, é mostrar que, seja qual for o número natural n, $21n + 4$ e $14n + 3$ não têm fator primo em comum.

Procedamos por contradição. Suponhamos, por absurdo, que n é um número natural tal que $21n + 4$ e $14n + 3$ têm um fator primo em comum. Chamemos esse fator primo de p. Na prática, então, estamos supondo que existem um natural n e um primo p tais que

$$21n + 4 \equiv 0 \pmod p \quad \text{e} \quad 14n + 3 \equiv 0 \pmod p,$$

e queremos chegar a uma contradição.

Multiplicando a primeira congruência por 2 e a segunda por 3, ficamos com

$$42n + 8 \equiv 0 \pmod p \quad \text{e} \quad 42n + 9 \equiv 0 \pmod p.$$

A primeira é equivalente a $42n \equiv -8 \pmod p$. A segunda, a $42n \equiv -9 \pmod p$. Dessa forma, temos $-8 \equiv -9 \pmod p \iff 9 - 8 \equiv 0 \pmod p \iff 1 \equiv 0 \pmod p$. Absurdo, pois não existe número primo que divida 1!

15. (a) Consideremos os possíveis casos:

- se $n \equiv 0 \pmod 3$, $n^3 - n \equiv 0 - 0 \equiv 0 \pmod 3$;
- se $n \equiv 1 \pmod 3$, $n^3 - n \equiv 1 - 1 \equiv 0 \pmod 3$;
- se $n \equiv 2 \pmod 3$, $n^3 - n \equiv 8 - 2 \equiv 6 \equiv 0 \pmod 3$.

Dessa forma, $n^3 - n$ é sempre divisível por 3.

(b) Queremos mostrar que $5 \mid n(n^4 - 1)$. Quando $n \equiv 0 \pmod 5$, o resultado é evidente. Nos outros casos, mostraremos que $5 \mid n^4 - 1$. Utilizaremos um pequeno truque: o fato de que $(-n)^4 \equiv n^4 \pmod 5$. Em função disso, é suficiente checar para $n \equiv 1 \pmod 5$ e $n \equiv 2 \pmod 5$:

- se $n \equiv 1 \pmod 5$, $n^4 - 1 \equiv 1 - 1 \equiv 0 \pmod 5$;
- se $n \equiv 2 \pmod 5$, $n^4 - 1 \equiv 16 - 1 \equiv 0 \pmod 5$.

Dessa forma, $n^5 - n$ é sempre divisível por 5.

(c) Queremos mostrar que $7 \mid n(n^6 - 1)$. Quando $n \equiv 0 \pmod 7$, o resultado é evidente. Nos outros casos, mostraremos que $7 \mid n^6 - 1$. Utilizaremos um pequeno truque: o fato de que $(-n)^6 \equiv n^6 \pmod 7$. Em função disso, é suficiente checar para $n \equiv 1 \pmod 7$, para $n \equiv 2 \pmod 7$ e para $n \equiv 3 \pmod 7$:

- se $n \equiv 1 \pmod 7$, $n^6 - 1 \equiv 1 - 1 \equiv 0 \pmod 7$;
- se $n \equiv 2 \pmod 7$, $n^6 - 1 \equiv 64 - 1 \equiv 0 \pmod 7$;
- se $n \equiv 3 \pmod 7$, $n^6 - 1 \equiv 3^6 - 1 \equiv 9^3 - 1 \equiv 2^3 - 1 \equiv 8 - 1 \equiv 0 \pmod 7$.

Dessa forma, $n^7 - n$ é sempre divisível por 7.

16. Temos $3^6 \equiv 9^3 \equiv (-1)^3 \equiv -1 \pmod 5$.
Além disso, $2^6 \equiv 64 \equiv -1 \pmod 5$.
Logo, $3^{6n} - 2^{6n} \equiv (-1)^n - (-1)^n \equiv 0 \pmod 5$.
Analisemos agora a divisibilidade por 7.
Temos $3^6 \equiv 9^3 \equiv 2^3 \equiv 1 \pmod 7$.
Além disso, $2^6 \equiv 8^2 \equiv 1^2 \equiv 1 \pmod 7$.
Logo, $3^{6n} - 2^{6n} \equiv 1^n - 1^n \equiv 0 \pmod 7$.
Dessa forma, $3^{6n} - 2^{6n}$ é divisível tanto por 5 quanto por 7, seja qual for o inteiro positivo n. Como $\text{mdc}(5, 7) = 1$, segue que $3^{6n} - 2^{6n}$ é divisível pro $5 \times 7 = 35$, seja qual for $n \in \mathbb{Z}$.

17. Consideremos os dois casos.

Caso I: $2^n - 1$ é primo.
Como $n > 2$, $2^n - 1 > 3$. Logo, se $2^n - 1$ é primo, $2^n - 1 \not\equiv 0 \pmod 3$.
Além disso, é claro que $2^n - 1 \not\equiv -1 \pmod 3$, já que $2^n \not\equiv 0 \pmod 3$.
Assim, $2^n - 1 \equiv 1 \pmod 3$ e, portanto, $2^n + 1 \equiv 3 \equiv 0 \pmod 3$.
Segue daí que $2^n + 1$ não é primo.

Caso II: $2^n + 1$ é primo.
Como $n > 2$, $2^n + 1 > 3$. Logo, se $2^n + 1$ é primo, $2^n + 1 \not\equiv 0 \pmod 3$.
Além disso, é claro que $2^n + 1 \not\equiv 1 \pmod 3$, já que $2^n \not\equiv 0 \pmod 3$.
Assim, $2^n + 1 \equiv -1 \pmod 3$ e, portanto, $2^n - 1 \equiv -3 \equiv 0 \pmod 3$.
Como $2^n - 1 > 3$, segue daí que $2^n - 1$ não é primo.

18. Suponhamos que o primo p é tal que $8p-1$ também é primo.

Se $p=3$, $8p+1=25$ é composto. Consideremos, então, daqui para a frente, que $p\neq 3$.

Temos $p\not\equiv 0 \pmod 3$ e $8p-1\not\equiv 0 \pmod 3 \iff -p-1\not\equiv 0 \pmod 3 \iff p\not\equiv -1 \pmod 3$. Logo, $p\equiv 1 \pmod 3$.

Assim, $8p+1\equiv 1+2=3\equiv 0 \pmod 3$ e, portanto, $8p+1$ não pode ser primo.

19. Suponhamos que o primo p é tal que $8p^2+1$ também é primo.

Se $p\not\equiv 0 \pmod 3$, $p^2\equiv 1 \pmod 3$ e, assim, $8p^2+1\equiv 8+1\equiv 9\equiv 0 \pmod 3$. Mas $8p^2+1>3$, donde, sendo primo, $8p^2+1$ não pode ser divisível pro 3. Logo, devemos ter $p\equiv 0 \pmod 3$.

Como p é primo, a única maneira de termos $p\equiv 0 \pmod 3$ é que tenhamos $p=3$. Assim, $p=3$, e $8p^2-1=71$ também é primo.

20. Observe que $n^2+3n+5=n^2+3n-28+33=(n+7)(n-4)+33$.

Assim, se n^2+3n+5 é divisível por 121, n^2+3n+5 é, em particular, divisível por 11 e, como 33 é divisível por 11, $(n+7)(n-4)$ também o deve ser.

Sendo 11 primo, $(n+7)(n-4)$ só pode ser divisível por 11 se $n+7$ ou $n-4$ o for. Veja agora que

$\to$ se $n+7\equiv 0 \pmod{11}$, então $n-4\equiv n+7-11\equiv 0 \pmod{11}$;

$\to$ se $n-4\equiv 0 \pmod{11}$, então $n+7\equiv n-4+11\equiv 0 \pmod{11}$.

Dessa forma, tanto $n+7$ quanto $n-4$ devem ser divisíveis por 11.

Daí, $(n+7)(n-4)$ deve ser divisível por $11\cdot 11=121$.

Logo, se $n^2+3n+5=(n+7)(n-4)+33$ for divisível por 121, 33 também o deve ser. Mas 33 não é divisível por 121. Portanto, não existe natural n para o qual n^2+3n+5 é divisível por 121.
