Aritmética dos Restos

Problemas com Congruências

Tópicos Adicionais

PORTAL DA MATEMÁTICA
OBMEP

Aritmética dos Restos
Problemas com Congruências

1 Exercícios Introdutórios

Exercício 1. Prove que $n^5 + 4n$ é divisível por 5 para todo inteiro n

Exercício 2. Prove que o número $n^3 + 2n$ é divisível por 3 para todo natural n.

Exercício 3. Prove que $n^2 + 1$ não é divisível por 3 para nenhum n inteiro.

Exercício 4. Dado o par de primos p e $p^2 + 2$, prove que $p^3 + 2$ também é um número primo.

Exercício 5. Prove que $n^3 + 2$ não é divisível por 9 para nenhum n inteiro.

Exercício 6. Se n não é múltiplo de 7, mostre que $n^3 \equiv \pm 1 \pmod 7$.

Exercício 7. Mostre que não existe inteiro m tal que $m^2 + 1 \equiv 0 \pmod 7$.

Exercício 8. Seja x um inteiro ímpar. Mostre que $x^4 \equiv 1 \pmod{16}$.

Exercício 9. Dados que $p, p + 10$ e $p + 14$ são números primos, encontre p.

Exercício 10. Mostre que $641 \mid 2^{32} + 1$.

2 Exercícios de Fixação

Exercício 11. Prove que $p^2 - 1$ é divisível por 24 se p é um primo maior que 3.

Exercício 12. Prove que $p^2 - q^2$ é divisível por 24 se p e q são primos maiores que 3.

Exercício 13. Seja $n > 6$ um inteiro positivo tal que $n - 1$ e $n + 1$ são primos. Mostre que $n^2(n^2 + 16)$ é divisível por 720. A recíproca é verdadeira?

Exercício 14. Prove que se $2n + 1$ e $3n + 1$ são ambos quadrados perfeitos, então n é divisível por 40.

Exercício 15. Se n é ímpar, prove que $7 | 2^{2n+1} + 3^{n+2}$.

Exercício 16. Para os inteiros positivos a, m e n, com $m \neq n$ e a par, mostre que

$$mdc(a^{2^n} + 1, a^{2^m} + 1) = 1.$$

Exercício 17. Mostre que, para todo $n \in \mathbb{N}$, que

a) $8 \mid 3^{2n} + 7$.

b) $a^2 + a + 1 \mid (a + 1)^{2n+1} + a^{n+2}$, para todo $a \in \mathbb{N}$.

3 Exercícios de Aprofundamento e de Exames

Exercício 18. Achar o menor natural n tal que 2001 é a soma dos quadrados de n inteiros ímpares.

Exercício 19. Seja $s(n)$ a soma dos dígitos de n. Se $N = 4444^{4444}$, $A = s(N)$ e $B = s(A)$. Quanto vale $s(B)$?

Exercício 20. Prove que $11^{n+2} + 12^{2n+1}$ é divisível por 133 para qualquer natural n.

Exercício 21. Seja $d(n)$ a soma dos dígitos de n. Suponha que $n + d(n) + d(d(n)) = 1995$. Quais os possíveis restos da divisão de n por 9?

Exercício 22. Prove que não existem inteiros positivos $x_1, x_2, \ldots, x_{14}$ tais que:

$$x_1^4 + x_2^4 + \ldots + x_{14}^4 = 1599.$$

Exercício 23. Determine todos os primos p para os quais o sistema

$$p + 1 = 2x^2$$
$$p^2 + 1 = 2y^2$$

tem uma solução nos inteiros x, y.

Exercício 24. Mostre que para todo inteiro positivo n, existe um número de Fibonacci múltiplo de n.

Observação: A sequncia de Fibonacci é definida pela seguinte recursão:

$$F_{n+2} = F_{n+1} + F_n, \;\; n \in \mathbb{Z},$$

com $F_0 = 0$ e $F_1 = 1$.

Respostas e Soluções.

1. Inicialmente note que $n^5+4n = n(n^4+4)$. Se $n \equiv 0 \pmod 5$, não há o que fazer. Se $n \equiv \pm 1 \pmod 5$, $n^4+4 \equiv 1+4 = 0 \pmod 5$. Finalmente, se $n \equiv \pm 2 \pmod 5$, $n^2 \equiv 4 \equiv -1 \pmod 5$ e consequentemente $n^4+4 \equiv 1+4 = 0 \pmod 5$.

2. Se n não é múltiplo de 3, então $n \equiv \pm 1 \pmod 3$ e assim $n^2 \equiv 1 \pmod 3$. Daí, $n^2+2 \equiv 0 \pmod 3$. Se n é múltiplo de 3, $n \equiv 0 \pmod 3$. Em qualquer caso, $n(n^2+2) = n^3+2n$ é múltiplo de 3, pois é o produto de um inteiro e um múltiplo de 3.

3. Se n é múltiplo de 3, então $n^2+1 \equiv 0+1 \equiv 1 \pmod 3$. Se n não é múltiplo de 3, então

$$\begin{aligned} n &\equiv \pm 1 \pmod 3 \\ n^2 &\equiv (\pm 1)^2 \pmod 3 \\ n^2+1 &\equiv 2 \pmod 3. \end{aligned}$$

4. Se $p \neq 3$, pelo exercício anterior, $p^2+2 \equiv 0 \pmod 3$. Entretanto, como $p^2+2 > 3$, ele não seria um número primo. Logo, $p = 3$ e $p^3+2 = 29$, que é primo.

5. Podemos montar uma tabela de congruências na divisão por 9:

n	0	1	2	3	4	5	6	7	8
n^3	0	1	8	0	1	8	0	1	8

Como nenhum cubo perfeito deixa resto 7 na divisão por 9, $n^3+2 \not\equiv 0 \pmod 9$.

6. Podemos montar uma tabela de congruências na divisão por 7:

n	0	1	2	3	4	5	6
n^3	0	1	1	-1	1	-1	-1

7. Podemos montar uma tabela de congruências na divisão por 7:

n	0	1	2	3	4	5	6
n^2	0	1	4	2	2	4	1

Como nenhum quadrado deixa resto 6, não é possível que $n^2+1 \equiv 0 \pmod 7$.

Observação: Pelo exercício anterior, se m não é divisível por 7, então $m^6 = (m^3)^2 \equiv (\pm 1)^2 = 1 \pmod 7$. Por outro lado, se $m^2+1 \equiv 0 \pmod 7$, teremos $m^6 = (m^2)^3 \equiv (-1)^3 = -1 \pmod 7$. Ou seja, $1 \equiv -1 \pmod 7$. Isso é um absurdo, pois $7 \nmid 2$.

8. Se x é ímpar, então $x = 2k+1$. Daí $x^2 = 4k(k+1)+1 \equiv 1 \pmod 8$, pois $2 \mid k(k+1)$. Além disso, $x^2+1 \equiv 1 \pmod 2$. Daí

$$16 = 8 \cdot 2 \mid (x^2-1)(x^2+1) = x^4-1.$$

9. Temos $p(p+10)(p+14) \equiv p(p+1)(p+2) \equiv 0 \pmod 3$, pois p, $p+1$ e $p+2$ são inteiros consecutivos. Daí, pelo menos um dos três primos é 3. Como p é o menor deles, $p = 3$ e $p+10 = 13$ e $p+14 = 17$.

10. Como $641 = 2^7 \cdot 5 + 1 = 5^4 + 2^4$, segue que

$$\begin{aligned} 2^7 \cdot 5 &\equiv -1 \pmod{641} \\ (2^7 \cdot 5)^4 &\equiv (-1)^4 \pmod{641} \\ 2^{28} \cdot 5^4 &\equiv 1 \pmod{641} \\ 2^{28} \cdot (-2^4) &\equiv 1 \pmod{641} \\ 2^{32}+1 &\equiv 0 \pmod{641}. \end{aligned}$$

11. Se p é um primo maior que 3, $p \equiv \pm 1 \pmod 3$ e $p \equiv 1 \pmod 2$. Daí, $p^2 \equiv 1 \pmod 3$. Além disso, se $p = 2k+1$, segue que $p^2 = 4k(k+1)+1 \equiv 1 \pmod 8$, pois $k(k+1)$ é par. Como $mdc(8,3) = 1$ e ambos dividem p^2-1, segue que $24 \mid p^2-1$.

12. Pelo exercício anterior,

$$\begin{aligned} p^2-q^2 &\equiv (p^2-1)-(q^2-1) \pmod{24} \\ &\equiv 0-0 \pmod{24} \\ &\equiv 0. \end{aligned}$$

13. (Extraído da Olimpíada Britânica) Veja que n é da forma $6k$, pois $n-1$ e $n+1$ são primos maiores que 3, portanto da forma $6k-1$ e $6k+1$, respectivamente. Logo,

$$n^2(n^2+16) = 144(9k^4+4k^2).$$

Resta provar que $9k^4+4k^2$ é um múltiplo de 5. Vamos analisar a igualdade acima módulo 5.

i) Se $k \equiv 0, 2$ ou $3 \pmod 5$, temos $9k^4+4k^2 \equiv 0 \pmod 5$;

ii) Se $k \equiv 1 \pmod 5 \Rightarrow n \equiv 1 \pmod 5$, temos $n-1 \equiv 0 \pmod 5$, um absurdo;

iii) Se $k \equiv 4 \pmod 5 \Rightarrow n \equiv 4 \pmod 5$, temos $n+1 \equiv 0 \pmod 5$, novamente um absurdo.

Isso conclui a demonstração. A recíproca não é verdadeira. Basta tomar, por exemplo, $n = 90$.

14. Podemos montar uma tabela de congruências na divisão por 5:

n	0	1	2	3	4
n^2	0	1	4	4	1
$2n+1$	1	3	0	2	4
$3n+1$	1	4	2	0	3

A segunda linha mostra que os únicos restos possíveis de um quadrado perfeito na divisão por 5 estão em $\{0, 1, 4\}$. Veja que $2n+1$ e $3n+1$ só admitem restos nesse conjunto simultaneamente quando $n \equiv 0 \pmod 5$. Podemos montar também uma tabela de congruências na divisão por 8:

n	0	1	2	3	4	5	6	7
n^2	0	1	4	1	0	1	0	1
$2n+1$	1	3	5	7	1	3	5	7
$3n+1$	1	4	7	2	5	0	3	6

O único caso em que simultaneamente $2n+1$ e $3n+1$ deixam o resto de um quadrado perfeito na divisão por 8 é quando $n \equiv 0 \pmod 8$. Como $mdc(8,5) = 1$, segue que $n \equiv 0 \pmod 4$0.

15.

$$\begin{aligned} 2^{2n+1} + 3^{n+2} &\equiv 4^n \cdot 2 + 3^n \cdot 9 \\ &\equiv (-3)^n \cdot 2 + 3^n \cdot 2 \\ &\equiv 0 \pmod 7. \end{aligned}$$

16. Suponha, sem perda de generalidade, que $m < n$ e seja p um divisor primo de $a^{2^n} + 1$ e $a^{2^m} + 1$. Claramente $p \neq 2$. Daí,

$$\begin{aligned} a^{2^m} &\equiv -1 \pmod p \\ (a^{2^m})^{2^{n-m}} &\equiv (-1)^{2^{n-m}} \pmod p \\ a^{2^n} &\equiv 1 \pmod p \\ a^{2^n} + 1 &\equiv 2 \pmod p \\ 0 &\equiv 2 \pmod p. \end{aligned}$$

Isso é um absurdo, pois $p \neq 2$. Lodo o mdc procurado é 1.

17.

a)

$$\begin{aligned} 3^{2n} &= (3^2)^n \\ &\equiv 1^n \pmod 8 \\ &\equiv -7 \pmod 8 \\ 3^{2n} + 7 &\equiv 0 \pmod 8. \end{aligned}$$

b) Seja $m = a^2 + a + 1$. Daí

$$\begin{aligned} (a+1)^{2n+1} + a^{n+2} &= \\ ((a+1)^2)^n \cdot (a+1) + a^2 \cdot a^n &= \\ (m+a)^n \cdot (a+1) + (m-a-1) \cdot a^n &= \\ a^n \cdot (a+1) - (a+1) \cdot a^n &\equiv 0 \pmod m. \end{aligned}$$

18. (Extraído da Olimpíada Cearense) Todo inteiro ímpar ao quadrado deixa resto 1 por 8. Usemos isso para estimar o valor de n. Sejam $x_1, x_2, \ldots, x_n$ inteiros ímpares tais que:

$$x_1^2 + x_2^2 + \ldots x_n^2 = 2001.$$

Analisando a congruência módulo 8, obtemos:

$$\begin{aligned} x_1^2 + x_2^2 + \ldots x_n^2 &= 2001 \pmod 8 \\ 1 + 1 + \ldots + 1 &\equiv 1 \pmod 8 \\ n &\equiv 1 \pmod 8) \end{aligned}$$

Como 2001 não é quadrado perfeito, não podemos ter $n = 1$. O próximo candidado para n seria $1 + 8 = 9$. Se exibirmos um exemplo para $n = 9$, teremos achado o valor mínimo. Veja que:

$$2001 = 43^2 + 11^2 + 5^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2.$$

19. (Extraído da Olimpíada Internacional) Pelo critério de divisibilidade por 9, $N \equiv A \equiv B \pmod 9$. Inicialmente calculemos o resto de N por 9. Como $4444 \equiv 16 \equiv 7 \pmod 9$, precisamos encontrar $7^{4444} \pmod 9$. Seguindo os métodos dos primeiros exemplos, seria interessante encontrarmos um inteiro r tal que $7^r \equiv \pm 1 \pmod 9$. O menor inteiro positivo com essa propriedade é $r = 3$. Como $4444 = 1481 \cdot 3 + 1$, temos:

$$7^{4444} \equiv 7^{1481 \cdot 3 + 1} \equiv (7^3)^{1481} \cdot 7 \equiv 7 \pmod 9.$$

Nosso próximo passo é estimar o valor de $s(B)$. Como $N = 4444^{4444} < 10^{5 \cdot 4444}$, $A = s(N) \leq 5 \cdot 4444 \cdot 9 = 199980$. Além disso, $B = s(A) \leq 1 + 9 \cdot 5 = 46$ e $s(B) \leq 12$. O único inteiro menor ou igual a 12 com resto 7 por 9 é o próprio 7, daí $s(B) = 7$.

20. (Extraído da Vídeo Aula) Duas relações que podemos extrair dos números envolvidos são: $144 - 11 = 133$ e $133 - 12 = 121$. Assim:

$$\begin{aligned} 144 &\equiv 11 \pmod{133}, \\ 12^2 &\equiv 11 \pmod{133}, \\ 12^{2n} &\equiv 11^n \pmod{133}, \\ 12^{2n+1} &\equiv 11^n \cdot 12 \pmod{133}, \\ 12^{2n+1} &\equiv 11^n \cdot (-121) + 133 \cdot 11^n \pmod{133}, \\ 12^{2n+1} &\equiv -11^{n+2} \pmod{133}. \end{aligned}$$

21. Seja r o resto na divisão por 9 de n. Pelo critério de divisibilidade por 9, temos:

$$n + d(n) + d(d(n)) \equiv 3r \equiv 1995 \pmod 9.$$

Assim, $r \equiv 2 \pmod 3$. Além disso,

$$\begin{aligned} n &\leq 1995 \Rightarrow \\ d(n) &\leq 27 = d(1989) \Rightarrow \\ d(d(n)) &\leq 10 = d(19). \end{aligned}$$

Consequentemente, $n \geq 1995 - d(n) - d(d(n)) \geq 1958$. Basta procurarmos no conjunto $\{1958, 1959, \ldots, 1995\}$ os inteiros que deixam resto 2 por 3 e que satisfazem a equação do problema. Nesse conjunto, apena o inteiro 1967 cumpre essas condições.

22. Estudando a congruência módulo 16, podemos mostrar que $x^4 \equiv 0$ ou $1 \pmod{16}$. Assim, a soma

$$x_1^4 + x_2^4 + \ldots + x_{14}^4$$

é congruente a um dos números do conjunto $\{0, 1, \ldots, 14\}$ módulo 16 enquanto que $1599 \equiv 15 \pmod{16}$. Um absurdo.

23. (Extraído da Olimpíada Alemã) Suponha sem perda de generalidade que $x, y \geq 0$. Como $p + 1$ é par, $p \neq 2$. Além disso,

$$2x^2 \equiv 1 \equiv 2y^2 \pmod{p}$$

e, consequentente, usando que p é ímpar, $x \equiv \pm y \pmod{p}$. Como $x < y < p$, temos

$$p^2 + 1 = 2(p - x)^2 = 2p^2 - 4px + p + 1,$$

de modo que $p = 4x - 1, 2x^2 = 4x$. Podemos concluir que x é 0 ou 2 e que a única possibilidade para p é $p = 7$.

24. Dado n, Analisemos os pares de restos possíveis entre números de Fibonacci consecutivos. Como existe apenas um número finito de pares de restos, um deles irá se repetir. Digamos que, para $s < t$, tenhamos

$$\begin{array}{ll} F_s \equiv a \pmod{n} & F_{s+1} \equiv b \pmod{n} \\ F_t \equiv a \pmod{n} & F_{t+1} \equiv b \pmod{n} \end{array}$$

Daí,

$$\begin{aligned} F_{s-1} &= F_{s+1} - F_s \\ &\equiv F_{t+1} - F_t \pmod{n} \\ &= F_{t-1} \end{aligned}$$

Suponha que, para $k \in \mathbb{Z}$, tenhamos

$$F_{s-k} \equiv F_{t-k} \pmod{n}. \text{ e } F_{s-(k-1)} \equiv F_{t-(k-1)} \pmod{n}$$

Daí,

$$\begin{aligned} F_{s-(k+1)} &= F_{s-(k-1)} - F_{s-k} \\ &\equiv F_{t-(k-1)} - F_{t-k} \pmod{n} \\ &= F_{t-(k+1)} \end{aligned}$$

Segue, por indução, que

$$F_{s-k} \equiv F_{t-k} \pmod{n}$$

para todo inteiro positivo k. Escolhendo $s = k$, temos

$$0 = F_0 \equiv F_{t-s} \pmod{n}.$$

Ou seja, $n \mid F_{t-s}$. De modo análogo, podemos mostrar que

$$F_{s+k} \equiv F_{t+k} \pmod{n}$$

para todo inteiro k. Fazendo $k = l(t - s) - s$, segue que

$$F_{l(t-s)} \equiv F_{(l-1)(t-s)} \pmod{n}$$

Assim, todos os números da sequência $\{F_{l(t-s)}\}_{l \in \mathbb{N}}$ são múltiplos de n.

Produzido por Arquimedes Curso de Ensino
contato@cursoarquimedes.com