Aritmética dos Restos

Aritmética Modular

Tópicos Adicionais

Aritmética dos Restos
Aritmética Modular

1 Exercícios Introdutórios

Exercício 1. Em cada item, encontre o menor inteiro positivo x que satisfaz as congruências:

(a) $x \equiv -5 \pmod 7$.

(b) $x \equiv -3 \pmod{11}$.

(c) $x \equiv -1 \pmod{13}$.

(d) $x \equiv 13 \pmod 7$.

(e) $x \equiv 27 \pmod 6$.

Exercício 2.

(a) Encontre o resto de $100 \cdot 103 \cdot 104$ na divisão por 7.

(b) Encontre o resto de $100^2 \cdot 102$ na divisão por 9.

(c) Encontre o resto de $37^3 \cdot 2$ na divisão por 3.

(d) Encontre o resto de $98 \cdot 101$ na divisão por 11.

Exercício 3. Determine o inverso de 11 nos seguintes módulos: 3, 5, 7 e 9.

Exercício 4. Encontre todos os inteiros x que satisfazem

(a) $2x \equiv 1 \pmod 7$

(b) $2x \equiv 3 \pmod 7$

(c) $3x \equiv 9 \pmod{13}$

(d) $5x \equiv 7 \pmod{13}$

Exercício 5. Observe os restos das potências de 2 na divisão por 3:

	2^0	2^1	2^2	2^3
Resto	1	2	1	2
	2^4	2^5	2^6	2^7
Resto	1	2	1	2

(a) Seguindo o padrão da tabela, qual deve ser o resto de 2^{2016} na divisão por 3?

(b) Verifique que $2^{2k} \equiv 1 \pmod 3$ e que $2^{2k+1} \equiv 2 \pmod 3$ para todo k inteiro não negativo.

Exercício 6. Calcule o resto de 4^{100} por 3.

Exercício 7. Calcule o resto de 4^{100} por 5.

Exercício 8. Calcule o resto de 4^{100} por 7.

Exercício 9. Determine o resto de $2^{20} - 1$ na divisão por 41.

2 Exercícios de Fixação

Exercício 10. Verifique que a sequência de restos das potências de 3 na divisão por 7 é periódica e determine o seu período, ou seja, o menor inteiro positivo k tal que 3^t e 3^{k+t} possuam o mesmo resto na divisão por 7 para todo o inteiro t não negativo.

Exercício 11. (a) Qual o resto de $2^{100} + 3^{100}$ por 7?

(b) Qual o resto de 444^{333} por 7?

(c) Qual o resto de $333^{777} + 777^{333}$ por 5?

Exercício 12. Qual o resto na divisão de $2^{70} + 3^{70}$ por 13?

Exercício 13. Qual o resto de 3^{200} por 100?

Exercício 14. Qual o último dígito de 777^{777}?

Exercício 15. Prove que $2222^{5555} + 5555^{2222}$ é divisível por 7.

Exercício 16. Escreva uma única congruência que é equivalente ao par de congruências $x \equiv 1 \pmod 4$ e $x \equiv 2 \pmod 3$.

3 Exercícios de Aprofundamento e de Exames

Exercício 17. Qual o resto de $36^{36} + 41^{41}$ na divisão por 77?

Exercício 18. Qual é a maior potência de 2 que divide $2011^{2012} - 1$?

Exercício 19. Qual o resto de $1^{2000} + 2^{2000} + \ldots + 2000^{2000}$ na divisão por 7?

Respostas e Soluções.

1.

(a) $x = 2$.

(b) $x = 8$.

(c) $x = 12$.

(d) $x = 6$.

(e) $x = 3$.

2.

(a) Como $100 \equiv 2 \pmod 7$, segue que

$$\begin{aligned} 100 \cdot 103 \cdot 104 &\equiv 2 \cdot 5 \cdot 6 \pmod 7 \\ &\equiv 60 \pmod 7 \\ &\equiv 4 \pmod 7. \end{aligned}$$

Portanto, o resto é 4.

(b) Como $100 \equiv 1 \pmod 9$, segue que

$$\begin{aligned} 100^2 \cdot 102 &\equiv 1^2 \cdot 3 \pmod 7 \\ &\equiv 3 \pmod 7 \end{aligned}$$

Portanto, o resto é 3.

(c) Como $37 \equiv 1 \pmod 3$, segue que

$$\begin{aligned} 37^3 \cdot 2 &\equiv 1^3 \cdot 2 \pmod 3 \\ &\equiv 2 \pmod 7 \end{aligned}$$

Portanto, o resto é 2.

(d) Como $98 \equiv 10 \pmod{11}$, segue que

$$\begin{aligned} 98 \cdot 101 &\equiv 10 \cdot 2 \pmod{11} \\ &\equiv 20 \pmod{11} \\ &\equiv 9 \pmod{11} \end{aligned}$$

Portanto, o resto é 9. Uma maneira alternativa seria:

$$\begin{aligned} 98 \cdot 101 &\equiv -1 \cdot 2 \pmod{11} \\ &\equiv -2 \pmod{11} \\ &\equiv 9 \pmod{11} \end{aligned}$$

3. Pelo Algoritmo de Euclides Estendido, como $mdc(11,3) = 1$, podemos encontrar a combinação linear:

$$11 \cdot 2 + 3 \cdot (-7) = 1.$$

Daí, $11 \cdot 2 \equiv 1 \pmod 3$. Procedendo de forma análoga, podemos encontrar:

$$\begin{aligned} 11 \cdot 1 &\equiv 1 \pmod 5 \\ 11 \cdot 2 &\equiv 1 \pmod 7 \\ 11 \cdot 5 &\equiv 1 \pmod 9. \end{aligned}$$

4.

(a) Como o inverso de $2 \pmod 7$ é 4, podemos multiplicar a congruência e obter:

$$\begin{aligned} 2x &\equiv 1 \pmod 7 \Leftrightarrow \\ 8x &\equiv 4 \pmod 7 \Leftrightarrow \\ x &\equiv 4 \pmod 7. \end{aligned}$$

Portanto, o inteiro x satisfaz a congruência dada se, e somente se, x deixa resto 4 na divisão por 7.

(b) Procedendo como no exercício anterior, dado que $2 \cdot 4 \equiv 1 \pmod 7$, a resposta é

$$\begin{aligned} 2x &\equiv 3 \pmod 7 \Leftrightarrow \\ 8x &\equiv 12 \pmod 7 \Leftrightarrow \\ x &\equiv 5 \pmod 7. \end{aligned}$$

(c) Como $3 \cdot 9 \equiv 1 \pmod{13}$, temos

$$\begin{aligned} 3x &\equiv 9 \pmod{13} \Leftrightarrow \\ 27x &\equiv 81 \pmod{13} \Leftrightarrow \\ x &\equiv 3 \pmod{13}. \end{aligned}$$

(d) Como $5 \cdot 8 \equiv 1 \pmod{13}$, temos

$$\begin{aligned} 5x &\equiv 7 \pmod{13} \Leftrightarrow \\ 40x &\equiv 56 \pmod{13} \Leftrightarrow \\ x &\equiv 4 \pmod{13}. \end{aligned}$$

5.

(a) Seguindo a tabela anterior, potências de 2 com expoente par sempre deixam resto 1 na divisão por 3. Portanto, caso o padrão seja mantido, 2^{2016} deve deixar resto 1 na divisão por 3.

(b) Como $2^2 \equiv 1 \pmod 3$, elevando ambos os lados da congruência a potência k, temos $2^{2k} = (2^2)^k \equiv 1^k = 1 \pmod 3$. Além disso, multiplicando a última congruência por 2, obtemos:

$$\begin{aligned} 2 \cdot 2^{2k} &\equiv 2 \cdot 1 \pmod 3 \\ 2^{2k+1} &\equiv 2 \pmod 3. \end{aligned}$$

6. Como $4 \equiv 1 \pmod 3$, temos $4^{100} \equiv 1^{100} = 1 \pmod 3$. Outra solução é usar o exercício anterior e perceber que $4^{100} = 2^{200} \equiv 1 \pmod 3$, pois 200 é par.

7. Como $4 \equiv -1 \pmod 5$, temos $4^{100} \equiv (-1)^{100} = 1 \pmod 5$.

8. Você deve ter percebido que encontrar relações do tipo $a \equiv \pm 1 \pmod m$ podem simplificar bastante o cálculo de $a^k \pmod m$. Procuremos alguma relação como essa para 4 e 7. Veja que:

$$\begin{aligned} 4^0 &\equiv 1 \pmod 7 \\ 4^1 &\equiv 4 \pmod 7 \\ 4^2 &\equiv 2 \pmod 7 \\ 4^3 &\equiv 1 \pmod 7. \end{aligned}$$

Assim,

$$\begin{aligned} 4^{99} &= (4^3)^{33} \\ &\equiv 1^{33} \pmod 7 \\ &\equiv 1 \pmod 7 \\ 4^{100} &\equiv 4 \pmod 7. \end{aligned}$$

Portanto, o resto é 4.

Observação: Como $4^3 \equiv 1 \pmod 7$, os restos das potências de 4 na divisão por 7 se repetem periodicamente de 3 em 3, pois $4^{3k+r} \equiv 4^{3k} \cdot 4^r \equiv 4^r \pmod 7$. Outra abordagem é perceber que $2^3 \equiv 1 \pmod 7$. Daí,

$$\begin{aligned} 4^{99} &= 2^{198} \\ &= (2^3)^{66} \\ &\equiv 1^{66} \pmod 7. \end{aligned}$$

9. Veja que

$$\begin{aligned} 2^5 = 32 &\equiv -9 \pmod{41} \Rightarrow \\ 2^{10} \equiv 81 &\equiv -1 \pmod{41} \Rightarrow \\ 2^{20} &\equiv 1 \pmod{41}. \end{aligned}$$

Assim, o resto procurado é zero.

10. Considere a sequência de restos:

$$\begin{aligned} 3^0 &\equiv 1 \pmod 7 \\ 3^1 &\equiv 3 \pmod 7 \\ 3^2 &\equiv 2 \pmod 7 \\ 3^3 &\equiv -1 \pmod 7 \\ 3^4 &\equiv -3 \pmod 7 \\ 3^5 &\equiv -2 \pmod 7 \\ 3^6 &\equiv 1 \pmod 7 \end{aligned}$$

Como $3^6 \equiv 1 \pmod 7$, segue que $3^{t+6} \equiv 3^t \cdot 3^6 \equiv 3^t \pmod 7$ para todo t não negativo. Além disso, em virtude da tabela anterior, nenhum número positivo menor que 6 pode ter essa propriedade. Portanto, o período é 6.

11.

(a)

$$\begin{aligned} 2^{100} + 3^{100} &= (2^3)^{33} \cdot 2 + (3^3)^{33} \\ &\equiv 1^{33} \cdot 2 + (-1)^{33} \cdot 3 \pmod 7 \\ &\equiv -1 \pmod 7 \\ &\equiv 6 \pmod 7. \end{aligned}$$

Portanto, o resto é 6.

(b)

$$\begin{aligned} 444^{333} &\equiv 3^{777} \pmod 7 \\ &\equiv (3^3)^{259} \pmod 7 \\ &\equiv (-1)^{259} \pmod 7 \\ &\equiv -1 \pmod 7 \\ &\equiv 6 \pmod 7 \end{aligned}$$

Portanto, o resto é 6.

(c)

$$\begin{aligned} 333^{777} + 777^{333} &\equiv 3^{777} + 7^{333} \pmod 5 \\ &\equiv (3^2)^{388} \cdot 3 + (7^2)^{166} \cdot 7 \pmod 5 \\ &\equiv (-1)^{388} \cdot 3 + (-1)^{166} \cdot 7 \pmod 5 \\ &\equiv 3 + 7 \pmod 5 \\ &\equiv 0 \pmod 5. \end{aligned}$$

Portanto, o resto é 0.

12. Como $13 = 4 + 9$, podemos escrever:

$$\begin{aligned} 9 &\equiv -4 \pmod{13} \Rightarrow \\ 9^{35} &\equiv (-4)^{35} \pmod{13} \Rightarrow \\ 3^{70} + 2^{70} &\equiv 0 \pmod{13}. \end{aligned}$$

13. Analisemos os restos na divisão por 100 de 3^k:

$$\begin{aligned} 3^1 &\equiv 03 \pmod{100} \\ 3^2 &\equiv 09 \pmod{100} \\ 3^3 &\equiv 27 \pmod{100} \\ 3^4 &\equiv 81 \pmod{100} \\ 3^5 &\equiv 43 \pmod{100} \\ 3^6 &\equiv 29 \pmod{100} \\ 3^7 &\equiv 87 \pmod{100} \\ 3^8 &\equiv 61 \pmod{100} \\ 3^9 &\equiv 83 \pmod{100} \\ 3^{10} &\equiv 49 \pmod{100} \end{aligned}$$

Como $49 = 50 - 1$, temos

$$\begin{aligned} 3^{20} &\equiv (50-1)^2 \pmod{100} \\ &\equiv 2500 - 100 + 1 \pmod{100} \\ &\equiv 1 \pmod{100} \end{aligned}$$

Finalmente,

$$\begin{aligned} 3^{200} &= (3^{20})^{10} \pmod{100} \\ &\equiv 1^{10} \pmod{100} \\ &\equiv 1 \pmod{100}. \end{aligned}$$

Observação: Outra abordagem é perceber que

$$\begin{aligned} 3^{200} - 1 &= (3^{100} - 1)(3^{100} + 1) \\ &= (3^{50} - 1)(3^{50} + 1)(3^{100} + 1) \\ &= (3^{25} - 1)(3^{25} + 1)(3^{50} + 1)(3^{100} + 1) \end{aligned}$$

Todos os parênteses anteriores são números pares e, consequentemente, o produto resultante é um múltiplo de 8. Como

$$\begin{aligned} 3^3 &\equiv 2 \pmod{25} \\ (3^3)^4 &\equiv 2^4 \pmod{25} \\ 3^{12} &\equiv -3^2 \pmod{25}. \end{aligned}$$

Ou seja, $25 \mid 3^2(3^{10}+1)$. Sabendo que $mdc(25,3^2)=1$, temos $25 \mid 3^{10}+1$. Daí $3^{50} \equiv (-1)^5 \equiv -1 \pmod 2)5$. Assim, $25 \mid 3^{50}+1$. Como 8 e 25 dividem $3^{200}-1$, podemos concluir que $3^{200}-$ é múltiplo de 200 e naturalmente termina em 00. Logo, 3^{200} termina em 01.

14. O último dígito é determinado pelo resto na divisão por 10.

$$\begin{aligned} 777^{777} &\equiv 7^{777} \pmod{10} \\ &\equiv (7^2)^{383}\cdot 7 \pmod{10} \\ &\equiv (-1)^{383}\cdot 7 \pmod{10} \\ &\equiv -7 \pmod{10} \\ &\equiv 3 \pmod{10} \end{aligned}$$

Portanto, o último dígito é 3

15. Como $2222+5555=7777$, que é um múltiplo de 7, temos

$$\begin{aligned} 2222^{5555}+5555^{2222} &\equiv (-5555)^{5555}+5555^{2222} \pmod 7 \\ &\equiv -5555^{2222}(5555^{3333}-1) \pmod 7 \end{aligned}$$

Como $7 \nmid 5555^{2222}$, basta mostrarmos que $7 \mid 5555^{3333}-1$. Dividindo 5555 por 7, obtemos resto 4. Daí,

$$\begin{aligned} 5555^{3333} &\equiv 4^{3333} \pmod 7 \\ &\equiv (4^3)^{1111} \pmod 7 \\ &\equiv 1^{1111} \pmod 7 \\ &\equiv 1 \pmod 7. \end{aligned}$$

Daí, $7 \mid 5555^{3333}-1$ e isso termina o problema.

16. Como $x \equiv 1 \pmod 4$, podemos escrever $x=4q+1$. Daí, $4q+1 \equiv 2 \pmod 3$, ou seja,

$$\begin{aligned} 4q+1 &\equiv 2 \pmod 3 \\ 4q &\equiv 1 \pmod 3 \\ q &\equiv 1 \pmod 3. \end{aligned}$$

A última congruência nos diz que $q=3k+1$. Assim, $x=4(3k+1)+1=12k+5$ e a congruência resultante é $x \equiv 5 \pmod{12}$.

17. Inicialmente devemos perceber que existe uma relação entre os números do problema: $36+41=77$. Assim:

$$\begin{aligned} -36 &\equiv 41 \pmod{77}, \\ (-36)^{41} &\equiv 41^{41} \pmod{77}, \\ 36^{36}(1-36^5) &\equiv 36^{36}+41^{41} \pmod{77}. \end{aligned}$$

Nosso próximo passo é encontrar o resto de 36^5 na divisão por 77. Como $36 \equiv 1 \pmod 7$, $36^5 \equiv 1 \pmod 7$. Além disso, $36 \equiv 3 \pmod 1)1$ produzindo $36^5 \equiv 3^5 \equiv 1 \pmod 1)1$. Como $mdc(7,11)=1$ e ambos dividem 36^5-1, podemos concluir que $77 \mid 36^5-1$. Logo, $36^{36}+41^{41}$ deixa resto 0 na divisão por 77.

18. (Extraído da OBM 2012) Usando a diferença de quadrados, podemos escrever

$$\begin{aligned} 2011^{2012}-1 &= (2011^{1006}-1)(2011^{1006}+1) \\ &= (2011^{503}-1)(2011^{503}+1)(2011^{1006}+1). \end{aligned}$$

Como $2011 \equiv -1 \pmod 4$, temos

$$\begin{aligned} 2011^{1006}+1 &\equiv (-1)^{1006}+1 \pmod 4 \\ &\equiv 2 \pmod 4 \\ 2011^{503}-1 &\equiv (-1)^{503}-1 \pmod 4 \\ &\equiv 2 \pmod 4. \end{aligned}$$

Assim, $2011^{1006}+1$ e $2011^{503}-1$ são múltiplos de 2, mas não de 4 e o produto entre eles possui dois fatores 2. Agora,

$$\begin{aligned} 2011^{503}+1 &\equiv 3^{503}+1 \pmod 8 \\ &\equiv (3^2)^{251}+1\cdot 3 \pmod 8 \\ &\equiv 1^{251}\cdot 3+1 \pmod 8 \\ &\equiv 4 \pmod 8. \end{aligned}$$

Portanto, $2011^{503}+1$ é múltiplo de 4, mas não de 8, ou seja, possui exatamente dois fatores 2. Finalmente, o número dado possui $2\cdot 2=4$ fatores 2 e a maior potência de 2 que o divide é 2^4.

19. Como $i^{2000} \equiv (i+7k)^{2000} \pmod 7$, podemos simplificar o problema calculando primeiramente o valor de:

$$1^{2000}+2^{2000}+3^{2000}+4^{2000}+5^{2000}+6^{2000}+7^{2000} \pmod 7.$$

Outra observação importante que simplificará o cálculo é perceber que $2^3 \equiv 1 \pmod 7$. Assim,

$$\begin{aligned} 2^{3k} &\equiv 1 \pmod 7 \\ 2^{3k+1} &\equiv 2 \pmod 7 \\ 2^{3k+2} &\equiv 4 \pmod 7. \end{aligned}$$

Usando isso e o fato de que 2000 é par, temos:

$$\begin{aligned} 1^{2000}+2^{2000}+3^{2000}+4^{2000} &+ \\ 5^{2000}+6^{2000}+7^{2000} &\equiv \\ 1^{2000}+2^{2000}+(-4)^{2000}+4^{2000} &+ \\ (-2)^{2000}+(-1)^{2000}+0^{2000} &\equiv \\ 1+4+2+2+4+1+0 &\equiv 0 \pmod 7. \end{aligned}$$

Dentre os primeiros 2000 naturais consecutivos, podemos formar 285 grupos de 7 números consecutivos cuja soma é múltipla de 7, em virtude da soma anterior. Os cinco números restantes possuem como resto na divisão por 7 o número:

$$\begin{aligned} 1996^{2000}+1997^{2000}+1998^{2000} &+ \\ 1999^{2000}+2000^{2000} &\equiv \\ 1+4+2+2+4 &\equiv \\ &\equiv 6 \pmod 7. \end{aligned}$$

Assim, o resto da soma na divisão por 7 é 6.