Matemática Discreta - Listas de Exercícios

Jorge Augusto Salgado Salhani

Novembro, 2022

1 Lista 5 - Aritmética Modular

1.1 Verifique a veracidade ou falsidade das seguintes afirmações:

(a) $7 \equiv 24 \pmod 5$

$$\begin{aligned} 6 &\equiv 1 \pmod 5 \implies 6(4) \equiv 1(4) \pmod 5 \implies \\ 24 &\equiv 4 \pmod 5 \implies 7 \equiv 4 \pmod 5 \implies 7 - 4 = n5 \end{aligned}$$

Falso!

(b) $529 \equiv -8 \pmod 3$

$$\begin{aligned} 1 &\equiv -8 \pmod 3 \implies -8 \equiv 1 \pmod 3 \implies \\ 529 &\equiv 1 \pmod 3 \implies 528 = 3n \end{aligned}$$

Verdadeiro!

(c) $33 \equiv 57 \pmod 6$

$$\begin{aligned} 33 &\equiv 57 \pmod 6 \implies 11(3) \equiv 19(3) \pmod{2}(3) \implies 11 \equiv 19 \pmod 2 \\ 1 &\equiv 19 \pmod 2 \implies 19 \equiv 1 \pmod 2 \\ 11 &\equiv 1 \pmod 2 \implies 10 = 2n \end{aligned}$$

Verdadeiro!

(d) $-12 \equiv -72 \pmod 8$

$$-12 \equiv -72 \pmod 8 \implies -6(2) \equiv -36(2) \pmod{4}(2) \implies -6 \equiv -36 \pmod 4 \implies -36 \equiv -6 \pmod 4$$
$$2 \equiv -6 \pmod 4 \implies -6 \equiv 2 \pmod 4$$
$$-36 \equiv 2 \pmod 4 \implies -18 \equiv 1 \pmod 2 \implies -19 = 2n$$

Falso!

(e) $-285 \equiv 27 \pmod 8$

$$27 \equiv 3 \pmod 8 \implies -285 \equiv 3 \pmod 8$$
$$3 \equiv -5 \pmod 8 \implies -285 \equiv -5 \pmod 8 \implies -57(5) \equiv -1(5) \pmod 8 \implies$$
$$-57 \equiv -1 \pmod 8 \implies -56 = 8n$$

Verdadeiro!

(f) $695 \equiv 22 \pmod 8$

$$22 \equiv -2 \pmod 8 \implies 695 \equiv -2 \pmod 8$$
$$695 - 24 \equiv 22 - 24 \pmod 8 \implies 671 \equiv -2 \pmod 8 \implies -2 \equiv 671 \pmod 8$$
$$695 \equiv 671 \pmod 8 \implies 24 = 8n$$

Verdadeiro! ERRADO!

1.2 Sejam a, b, c inteiros positivos tais que $a \equiv -1 \pmod 7$ e os restos da divisão por 7 de b e c são 6 e 3, respectivamente. Encontre o resto da divisão de $a + b + c$ por 7.

$$a \equiv -1 \pmod 7 \quad b \equiv 6 \pmod 7 \quad c \equiv 3 \pmod 7$$

$$a + b + c \equiv (-1 + 6 + 3) \pmod 7 \implies k \equiv 8 \pmod 7$$
$$8 \equiv 1 \pmod 7 \implies k \equiv 1 \pmod 7$$
$$a + b + c \equiv 1 \pmod 7$$

r = 1 ERRADO!

1.3 Calcule o resto da divisão de

(a) 7^{25} por 3

$$7 \equiv 1 \pmod 3 \implies 7^{25} \equiv 1^{25} \pmod 3 = 1 \pmod 3$$

r = 1 ERRADO!

(b) $17^{15689879}$ por 3

$$17 \equiv -1 \pmod 3 \implies 17^{15689879} \equiv (-1)^{15689879} \pmod 3 = -1 \pmod 3$$
$$2 \equiv -1 \pmod 3 \implies -1 \equiv 2 \pmod 3$$
$$17^{15689879} \equiv 2 \pmod 3$$

r = 2

(c) 23^{71355} por 4

$$23 \equiv -1 \pmod 4 \implies 23^{71355} \equiv (-1)^{71355} \pmod 4 = -1 \pmod 4$$
$$3 \equiv -1 \pmod 4 \implies -1 \equiv 3 \pmod 4$$
$$23^{71355} \equiv 3 \pmod 4$$

r = 3

1.4 Mostre que se $n \in \mathbb{N}$, então o algarismo das unidades na representação da base 10 de 3^n só pode ser 1,3,7 ou 9

$$3^n \equiv r \pmod{10} \quad r = \{1, 3, 7, 9\}$$

$$a$$

1.5 Ache o algarismo das unidades na representação da base 10 dos seguintes números

(a) 3^{2022}

$$
\begin{aligned}
9 &\equiv -1 \pmod{10} \implies 3^2 \equiv -1 \pmod{10} \\
(3^2)^{1011} &\equiv (-1)^{1011} \pmod{10} = -1 \pmod{10} \implies \\
3^{2022} &\equiv -1 \pmod{10} \\
9 &\equiv -1 \pmod{10} \implies -1 \equiv 9 \pmod{10} \\
3^{2022} &\equiv 9 \pmod{10}
\end{aligned}
$$

r = 9

(b) 3^{2003}

$$3^{2003} = 3^{2002+1} = 3^{2002}3$$

$$
\begin{aligned}
3^{2002} &= (3^2)^{1001} \\
3^2 &\equiv -1 \pmod{10} \implies (3^2)^{1001} \equiv (-1)^{1001} \pmod{10} \\
3^{2002} &\equiv -1 \pmod{10} \\
3 &\equiv -7 \pmod{10}
\end{aligned}
$$

$$
\begin{aligned}
3^{2002}3 &\equiv (-1)(-7) \pmod{10} \implies \\
3^{2002} &\equiv 7 \pmod{10}
\end{aligned}
$$

r = 7

(c) 3^{741}

$$3^{741} = 3^{740+1} = 3^{740}3$$

$$
\begin{aligned}
3^{740} &= (3^2)^{370} \\
3^2 &\equiv -1 \pmod{10} \implies (3^2)^{370} \equiv (-1)^{370} \\
3^{740} &\equiv 1 \pmod{10} \\
3 &\equiv -7 \pmod{10}
\end{aligned}
$$

$$
\begin{aligned}
3^{740}3 &\equiv -7 \pmod{10} \\
3 &\equiv -7 \pmod{10} \implies -7 \equiv 3 \pmod{10} \\
3^{741} &\equiv 3 \pmod{10}
\end{aligned}
$$

r = 3

1.6 Calcule o resto da divisão de

(a) 11^{p-1} por p, com p primo.

$$a^{p-1} \equiv 1 \pmod p \implies 11^{p-1} \equiv 1 \pmod p$$

r = 1

(b) 2^{100} por 11

$$\begin{aligned} 2^{100} &= (2^{11-1})^2 \\ 2^{11-1} &\equiv 1 \pmod{11} \implies (2^{11-1})^2 \equiv 1^2 \pmod{11} \implies \\ 2^{100} &\equiv 1 \pmod{11} \end{aligned}$$

r = 1

Por outro caminho...

$$2^{100} = 2^{99+1} = 2^{9(11)+1} = (2^9)^{11}2$$

$$\begin{aligned} a^p \equiv a \pmod p &\implies (2^9)^{11} \equiv 2^9 \pmod{11} = (2^3)^3 \pmod{11} \\ 2 &\equiv -9 \pmod{11} = -3(3) \pmod{11} \\ 2^{100} &= (2^9)^{11}2 \equiv (2^3)^3(-9) \pmod{11} \end{aligned}$$

$$\begin{aligned} 2^3 \equiv -3 \pmod{11} &\implies (2^3)^3 \equiv (-3)^3 \pmod{11} \implies \\ (2^3)^3 &\equiv (-1)^3(3)^3 \pmod{11} = -(3)^3 \pmod{11} \end{aligned}$$

$$\begin{aligned} -9 &\equiv 3 \pmod{11} \\ 2^{100} &\equiv -(3)^3 3 \pmod{11} \end{aligned}$$

$$\begin{aligned} 3^3 &\equiv 5 \pmod{11} \\ 3 &\equiv -8 \pmod{11} \end{aligned}$$

$$\begin{aligned} 2^{100} &\equiv -5(8) \pmod{11} = -40 \pmod{11} \\ -40 &\equiv 4 \pmod{11} \\ 2^{100} &\equiv 4 \pmod{11} \end{aligned}$$

(c) $20^{15} - 1$ por 11

$$20^{15} = 20^{11-1+5} = 20^{11-1}20^5$$

$$\begin{aligned}
20^{11-1} &\equiv 1 \pmod{11} \\
20 &\equiv -2 \pmod{11} \implies 20^5 \equiv -2^5 \pmod{11} \\
-2^5 &= -32 \implies -2^5 \equiv -1 \pmod{11} \\
20^5 &\equiv -1 \pmod{11}
\end{aligned}$$

$$\begin{aligned}
20^{15} &\equiv 1(-1) \pmod{11} = -1 \pmod{11} \implies \\
20^{15} - 1 &\equiv -2 \pmod{11} \\
-2 &\equiv 9 \pmod{11} \\
20^{15} - 1 &\equiv 9 \pmod{11}
\end{aligned}$$

r = 9 ERRADO!