Matemática Discreta - Listas de Exercícios

Jorge Augusto Salgado Salhani

Novembro, 2022

1 Lista 6 - Aritmética Modular

1.1 Calcule o conjunto $\mathcal{U}(n)$ dos elementos invertíveis de $\mathbb{Z}_n$ para os seguintes casos:

(a) $n = 3$

Sendo $a \in \mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$, se $\gcd(a, n) = 1$, então $a \in \mathcal{U}(n)$.

Dessa forma, sendo $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, então $\mathcal{U}(3) = \{\overline{1}, \overline{2}\}$.

(b) $n = 4$

$\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, então $\mathcal{U}(4) = \{\overline{1}, \overline{3}\}$.

c $n = 6$

$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, então $\mathcal{U}(6) = \{\overline{1}, \overline{5}\}$.

(d) $n = 8$

$\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$, então $\mathcal{U}(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

(e) $n = 11$

$\mathbb{Z}_{11} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}\}$. Então $\mathcal{U}(11) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}\}$

1.2 Encontre o inverso de cada elemento de $\mathcal{U}(n)$ da questão anterior.

(a) $n = 3$

$\mathcal{U}(3) = \{\overline{1}, \overline{2}\}$.

Seja b inverso de $\overline{a} \in \mathcal{U}(n)$, então

$$\gcd(a, n) = 1 \implies ax + ny = 1$$

com a implicação dada pela identidade de Bezout. Assim $ax \equiv 1 \pmod n$, com $x \equiv b \pmod n$, onde podemos encontrar x e y pelo algoritmo de Euclides.

Para $\overline{2}$,

$$2x + 3y = 1$$

$$\begin{aligned} 3 = 2(1) + 1 \implies 3 - 2(1) &= 1 \\ 3(1) + 2(-1) &= 1 \end{aligned}$$

$(x, y) = (-1, 2)$. Logo

$$-1 \equiv b \pmod 3 \implies -1 - b = 3k, k \in \mathbb{Z}$$

$b = \overline{2}$

(b) $n = 4$

$\mathcal{U}(4) = \{\overline{1}, \overline{3}\}$.

Para $\overline{3}$

$$3x + 4y = 1$$

$$\begin{aligned} 4 = 3(1) + 1 \implies 1 &= 4 - 3(1) \\ 4(1) + 3(-1) &= 1 \end{aligned}$$

$(x, y) = (-1, 1)$. Logo

$$-1 \equiv b \pmod 4 \implies -1 - b = 4k$$

$b = \overline{3}$.

(c) $n = 6$

$\mathcal{U}(6) = \{\overline{1}, \overline{5}\}$

$$5x + 6y = 1$$

$$6 = 5(1) + 1 \implies 1 = 6(1) - 5(1)$$
$$6(1) + 5(-1) = 1$$

$(x, y) = (-1, 1)$. Logo

$$-1 \equiv b \pmod 6 \implies -1 - b = 6k$$

$\bar{b} = 5$

(d) $n = 8$

$\mathcal{U}(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

Para $\overline{3}$

$$3x + 8y = 1$$

$$8 = 3(2) + 2$$
$$3 = 2(1) + 1$$

$$2 = 3 - 1 \implies 8 = 3(2) + (3 - 1) \implies$$
$$8 = 3(3) - 1 \implies 1 = 3(3) - 8 \implies 1 = 3(3) + 8(-1)$$

$(x, y) = (3, -1)$. Logo

$$3 \equiv b \pmod 8 \implies 3 - b = 8k \implies b = -5$$
$$-5 \equiv 3 \pmod 8 \implies b = 3$$

$\bar{b} = 3$

Para $\overline{5}$

$$5x + 8y = 1$$

$$8 = 5 + 3$$
$$5 = 3 + 2$$
$$3 = 2 + 1$$

$$1 = 3 - 2 = 3 - (5 - 3) = 3 - 5 + 3 = 3(2) - 5$$
$$3 = 8 - 5$$
$$1 = (8 - 5)(2) - 5 = 8(2) - 5(2) - 5 = 8(2) + 5(-3)$$

$(x, y) = (-3, 2)$. Logo

$$-3 \equiv b \pmod 8 \implies b \equiv -3 \pmod 8 \implies b + 3 = 8k$$

$b = \overline{5}$.

Para $\overline{7}$,

$$7x + 8y = 1 \tag{1}$$

$$8 = 7 + 1 \implies 1 = 8 - 7 = 8(1) + 7(-1)$$

$(x, y) = (-1, 1)$. Logo

$$-1 \equiv b \pmod 8 \implies b \equiv -1 \pmod 8 \implies b + 1 = 8k$$

$b = \overline{7}$.

(e) $n = 11$

$\mathbb{Z}_{11} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}\}$. Então $\mathcal{U}(11) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}\}$

Para $\overline{2}$,

$$2x + 11y = 1$$

$$11 = 5(2) + 1 \implies 1 = 11(1) - 2(5) = 11(1) + 2(-5)$$

$(x, y) = (-5, 1)$. Logo

$$-5 \equiv b \pmod{11} \implies b \equiv -5 \pmod{11} \implies b + 5 = 11k$$

$b = \overline{6}$

Para $\overline{3}$,

$$3x + 11y = 1$$

$$11 = 3(3) + 2$$
$$3 = 2 + 1$$

$$11 = 3(3) + (3-1) = 3(4) - 1 \implies$$
$$1 = 3(4) - 11 = 3(4) + 11(-1)$$

$(x, y) = (4, -1)$. Logo

$$4 \equiv b \pmod{11} \implies b = \overline{-7} = \overline{4}$$

$b = \overline{4}$

Para $\overline{5}$,

$$5x + 11y = 1$$

$$11 = 5(2) + 1 \implies 1 = 11(1) - 5(2) = 11(1) + 5(-2)$$

$(x, y) = (-2, 1)$, logo

$$-2 \equiv b \pmod{11} \implies -2 - b = 11k$$

$b = \overline{9}$

Para $\overline{10}$,

$$10x + 11y = 1$$

$$11 = 10(1) + 1 \implies 1 = 11(1) - 10(1) = 11(1) + 10(-1)$$

$(x, y) = (-1, 1)$. Logo

$$-1 \equiv b \pmod{11} \implies -1 - b = 11k$$

$b = \overline{10}$.

1.3 Para cada $\mathcal{U}(n)$ do exercício 1, encontre a(s) raiz(es) primitiva(s), se existir(em).

(a) $n = 3$

(b) $n = 4$

(c) $n = 6$

(d) $n = 8$

(e) $n = 11$

1.4 Determine a menor solução positiva de cada uma das congruências abaixo

(a) $x \equiv 7 \pmod{3}$

(b) $x \equiv -1 \pmod{6}$

(c) $3x \equiv 15 \pmod{4}$

(d) $3x + 2 \equiv 0 \pmod{7}$

(e) $2x - 1 \equiv 7 \pmod{15}$

1.5 Calcule a função $\Phi(x)$ de Euler abaixo.

(a) $\Phi(125)$

(a) $\Phi(16200)$

(a) $\Phi(10!)$