11. Classes de congruência

Dado um número natural n e um inteiro a, a classe de congruência de a módulo n é o conjunto

$$[a]_n = \{x \in \mathbb{Z} : x \equiv_n a\}.$$

Quando n está fixado e não há risco de confusão, podemos escrever apenas $\overline{a}$ em vez de $[a]_n$. Definimos o conjunto de todas as classes de congruência módulo n por

$$\mathbb{Z}_n = \{\overline{a} : a \in \mathbb{Z}\} = \left\{\overline{0}, \overline{1}, \dots, \overline{n-1}\right\}.$$

Definimos em $\mathbb{Z}_n$ uma operação de adição por

$$\overline{a} + \overline{b} = \overline{a+b}$$

e um produto por

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Chamamos inverso de um elemento $\overline{a}$ em $\mathbb{Z}_n$ a um elemento $\overline{a'}$ tal que

$$\overline{a} \cdot \overline{a'} = \overline{1}.$$

Se $\overline{a}$ admite inverso, dizemos que $\overline{a}$ é invertível. Dizemos que um elemento não nulo $\overline{a} \in \mathbb{Z}_n$ é um divisor de zero se existe um elemento não nulo $\overline{b} \in \mathbb{Z}_n$ tal que

$$\overline{a} \cdot \overline{b} = \overline{0}.$$

Algoritmo RSA

O algoritmo RSA é um algoritmo utilizado em criptografia de chave pública. Foi apresentado por Ronald Linn Rivest (1947-), Adi Shamir (1952-) e Leonard Adleman (1945-) no artigo *A method for obtaining digital signatures and public-key cryptosystems*.[1] Funciona da seguinte maneira:

Geração da chave. São escolhidos dois números primos distintos, p e q. Seja $n = pq$ e seja $\phi(n) = (p-1)(q-1)$. Seja e um natural tal que $1 < e < \phi(n)$ e mdc $(e, \phi(n)) = 1$. Seja d um natural, com $1 < d < \phi(n)$, tal que $\overline{d}$ é o inverso de $\overline{e}$ em $\mathbb{Z}_{\phi(n)}$, isto é

$$ed \equiv_{\phi(n)} 1.$$

O par (n, e) será a chave pública e o natural d será a chave privada.

Encriptar. Para encriptar uma mensagem que esteja codificada num número m tal que $0 < m < n$, encontramos um natural c, com $c < n$, tal que

$$c \equiv_n m^e,$$

isto é, calculamos em $\mathbb{Z}_n$ a classe $[m^e]_n$

Desencriptar. Para recuperar a mensagem inicial, calculamos a classe

$$\left[c^d\right]_n$$

e obtemos $[m]_n$

Códigos sobre um alfabeto, códigos de Hamming

Dado um conjunto $A = \{a_1, \dots, a_q\}$, um *código binário sobre A* é um conjunto C de sequências de elementos de A. Chamamos a A o *alfabeto* do código. Se $q = 2$, dizemos que C é um *código binário*; se $q = 3$, dizemos que C é um *código ternário*. Por simplicidade, podemos denotar uma sequência $(u_1, \dots, u_n) \in C$ por $u_1 \cdots u_n$ dispensando parêntesis e vígulas.

Por exemplo, o código Morse é um código binário sobre o conjunto $\{\cdot, -\}$ (um sinal curto e um sinal longo). O pedido de socorro SOS costuma ser denotado por

$$\cdots --- \cdots$$

em vez de

$$(\cdot, \cdot, \cdot)\ (-, -, -)\ (\cdot, \cdot, \cdot).$$

Se C é um subconjunto de A^n, para algum natural $n \geq 1$, isto é, se todas as sequências de C têm comprimento n, dizemos que C é um *código binário de comprimento n sobre A*.

[1] Ronald Linn Rivest, Adi Shamir, Leonard Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the Association for Computing Machinery **21** (1978), n.º 2, 120–126.

$\mathbb{Z}_n$

Conjunto de invertíveis de $\mathbb{Z}_n$ $\{1, 2, \dots, n-1\}$ se n é primo pois $mdc(K, 7) = 1$, $\forall\ K \neq 0$

$\{a\}$ se $a.a \equiv_n 1$, $\forall\ a \in \mathbb{Z}$

$\{a.b\}$ se $a.b \equiv_n 1$, $\forall\ a, b \in \mathbb{Z}$

Divisor de 0 em $\mathbb{Z}_n$:

- Um elemento a é divisor de zero em $\mathbb{Z}_n$ se existe um b tal que $a.b \equiv_n 0$
- Um elemento a é divisor de zero em $\mathbb{Z}_n$ se $mdc(a, n) > 1$, mas $a \neq n$

1. Se a é invertível em $\mathbb{Z}_n$, então $mdc(a, n) = 1$
2. Se $mdc(a, n) = 1$, então a é invertível em $\mathbb{Z}_n$
3. Logo, a é invertível em $\mathbb{Z}_n$ sse $mdc(a, n) = 1$

Encriptar $c \equiv_n m^e$

$0 < m < n$

$c < n$

Calculamos a classe $[m^e]_n$ em $\mathbb{Z}_n$

Para desencriptar calculamos a classe $[c^d]_n$ e obtemos $[m]_n$

Algoritmo RSA

$n = p \cdot q$ p, q números primos

$\varphi(n) = (p-1)(q-1)$

$1 < e < \varphi(n)$, $mdc(e, \varphi(n)) = 1$

$ed \equiv_{\varphi(n)} 1$, $d \in \mathbb{N}$ e $1 < d < \varphi(n)$

- O par (n, e) é a chave pública e o natural d será a classe privada
- $\bar{d}$ é o inverso de $\bar{e}$ em $\mathbb{Z}_{(\varphi(n))}$

Por exemplo, o ADN pode ser descrito por um código genético de comprimento 3 sobre o alfabeto $\{A, C, G, T\}$.

Para códigos binários, é habitual considerar o conjunto $\mathbb{Z}_2$ como alfabeto. Neste caso, para aligeirar a notação, costumamos escrever 0 e 1, em vez de $\overline{0}$ e $\overline{1}$, para representar os elementos de $\mathbb{Z}_2$. A um código que é subespaço vectorial de $(\mathbb{Z}_2)^n$ chamamos *código linear binário*. Dado um código linear binário C de comprimento n, uma matriz geradora de C é uma matriz cujas linhas, encaradas como elementos de $(\mathbb{Z}_2)^n$, formam uma base de C. Por exemplo, a matriz

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

é uma matriz geradora do código linear

$$\{0000,\ 1100,\ 0110,\ 1010\}.$$

O código dual de um código C é o conjunto

$$C^{\perp} = \{(u_1, \ldots, u_n) \in (\mathbb{Z}_2)^n : \\ \forall (v_1, \ldots, v_n) \in C, u_1 v_1 + \cdots + u_n v_n = 0\}.$$

Uma *matriz de paridade* H de um código linear C é uma matriz geradora do código $C^{\perp}$. Como consequência, os elementos de C são definidos pela equação matricial

$$HX = 0.$$

Dado um natural $r \geq 2$, um código binário de Hamming de comprimento $2^r - 1$ é um código que admite uma matriz de paridade cujas colunas são todos os elementos de $(\mathbb{Z}_2)^r$.

Exercícios e problemas

1. Construa as tabelas de adição e multiplicação de $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_6$, $\mathbb{Z}_7$ e $\mathbb{Z}_{12}$. Em cada caso, identifique os elementos invertíveis e os divisores de zero.

2. Calcule $\overline{2}^9$, $\overline{3}^9$, e $\overline{10}^9$ em $\mathbb{Z}_{11}$.

3. Calcule $\overline{2}^{10}$, $\overline{3}^{10}$, e $\overline{10}^{10}$ em $\mathbb{Z}_{11}$.

4. (a) Mostre que se p é primo e $0 < k < p$, então $\binom{p}{k}$ é múltiplo de p.

   (b) Dê exemplo de um par de naturais n e k, com $0 < k < n$ tal que $\binom{n}{k}$ não é múltiplo de n.

   (c) **Pequeno teorema de Fermat.** Utilizando o binómio de Newton e a alínea (4a), mostre que se p é primo, para qualquer natural m, $m^p - m$ é múltiplo de p. [*Sugestão*: use indução em m.] Justifique que, em $\mathbb{Z}_p$, temos a igualdade

   $$\overline{m}^{p-1} = \overline{1}.$$

   (d) Utilizando o binómio de Newton e a alínea (4a), mostre que em $\mathbb{Z}_p$,

   $$\left(\overline{a} + \overline{b}\right)^p = \overline{a}^p + \overline{b}^p.$$

5. Considere um natural $n \geq 2$. Mostre que $\overline{a}$ é invertível em $\mathbb{Z}_n$ se e só se a e n são primos entre si.

6. Calcule $\overline{3}^{19}$ em $\mathbb{Z}_{25}$.

7. **Exponenciação rápida.** Uma representação binária de um natural m é uma sequência $a_k a_{k_1} \cdots a_0$ tal que $a_0, \ldots, a_k \in \{0, 1\}$ e

   $$m = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0.$$

   (a) Encontre a representação binária de 19.

   (b) Calcule as potências $\overline{3}^2$, $\overline{3}^4$, $\overline{3}^8$, e $\overline{3}^{16}$ em $\mathbb{Z}_{25}$, usando o facto de que, para qualquer natural s, $\overline{3}^{2s} = \left(\overline{3}^s\right)^2$.

   (c) Utilizando os resultados das alíneas anteriores, calcule $\overline{3}^{19}$ em $\mathbb{Z}_{25}$.

8. Considere a chave pública $(33, 7)$ para o algoritmo RSA.

   (a) Faça a encriptação do número 30.

   (b) Calcule a chave privada d para o algoritmo RSA (é necessário descobrir os primos p e q).

   (c) Faça a desencriptação do número obtido na alínea (8a).

6. $\overline{3}^{19}$ em $\mathbb{Z}_{25}$ $\qquad 19 = 16+2+1$

Em $\mathbb{Z}_{25}$:

$\overline{3}^2 = \overline{9}$

$\overline{3}^4 = (\overline{3}^2)^2 = (\overline{9})^2 = \overline{81} = \overline{6}$

$\overline{3}^8 = (\overline{3}^4)^2 = \overline{6}^2 = \overline{36} = \overline{11}$

$\overline{3}^{16} = (\overline{3}^8)^2 = \overline{11}^2 = \overline{121} = \overline{21}$

$\overline{3}^{19} = \overline{3}^{16} . \overline{3}^2 . \overline{3}^1 =$

$= \overline{21} . \overline{9} . \overline{3}$

$= \overline{21} . \overline{27} = \overline{21} . \overline{2}$

$= \overline{42} = \overline{17}$

R: $\overline{3}^{19} = \overline{17}$ em $\mathbb{Z}_{25}$

8. a) $c \equiv_n m^e$

$(m = 30;\ e = 7;\ n = 33)$

$c \equiv_{33} 30^7$

$\overline{30} = -3$ em $\mathbb{Z}_{33}$

$(-3)^7 = (\overline{-3})^4 . (\overline{-3})^1 = \overline{-3} . \overline{9} . \overline{15} = \overline{-27} . \overline{15} = \overline{6} . \overline{15} = \overline{90} = \overline{24}$

$(\overline{-3})^2 = 9$

$(\overline{-3})^4 = ((\overline{-3})^2)^2 = \overline{9}.\overline{9} = \overline{81} = \overline{15}$

Logo $c \equiv_{33} 6$

Resposta de encriptação: $c = 24$

b) $n = 33$

$33 = 3.11$

$p = 3 \quad , \quad q = 11$

$\varphi(n) = (p-1)(q-1)$

$= (3-1)(11-1)$

$= 20$

$d.e \equiv_{\varphi(n)} 1$

$(e = 7\ ;\ \varphi(n) = 20)$

$7d \equiv_{20} 1$

$20 = 2.7 + 6$

$7 = 1.6 + 1$

$6 = 6.1 + 0$

$1 = 7 - 1.6$

$= 7 - 1.(20 - 2.7)$

$= 3.7 - 1.20$

R: $d = 3$

↳ Classe privada

c) A fórmula para desencriptação é:

$m \equiv_n c^d$

Em $\mathbb{Z}_{33}$ $\qquad m \equiv_{33} 24^3$

$\overline{24} = \overline{-9}$

↳ $m \equiv_{33} \overline{-9}^3$

$\overline{-9}^3 = \overline{-9}^2 . (\overline{-9}) = \overline{-15} . \overline{9} = \overline{-135} = \overline{30}$

$\overline{-9}^2 = \overline{81} = \overline{15}$

9. Considerando os primos $p = 47$ e $q = 43$ e a chave pública $(2021, 335)$, calcule a chave privada d para o algoritmo RSA. Com a ajuda de um computador, faça a encriptação e a desencriptação do número 999.

10. Descreva o código linear binário sobre $\mathbb{Z}_2$ que admite a seguinte matriz geradora:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

11. Descreva o código linear binário sobre $\mathbb{Z}_2$ que admite a seguinte matriz de paridade:

$$H = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

12. Descreva um código binário de Hamming de comprimento 7 (usando $r = 3$).

13. O código ISBN-10 é um código de comprimento 10 sobre o alfabeto

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathrm{X}\}.$$

Este alfabeto representa o corpo $\mathbb{Z}_{11}$, cada algarismo representa a sua classe de congruência, e a letra X representa a classe $\overline{10}$. Dados os primeiros 9 dígitos $u_1, \dots, u_9$, o dígito de controle u_{10} é calculado de tal forma que, em $\mathbb{Z}_{11}$,

$$\overline{u_1} + \overline{2} \cdot \overline{u_2} + \overline{3} \cdot \overline{u_3} + \overline{4} \cdot \overline{u_4} + \overline{5} \cdot \overline{u_5} + \overline{6} \cdot \overline{u_6} + \overline{7} \cdot \overline{u_7} + \overline{8} \cdot \overline{u_8} + \overline{9} \cdot \overline{u_9} + \overline{10} \cdot \overline{u_{10}} = \overline{0}.$$

(a) Os primeiros nove dígitos do identificador ISBN-10 de uma das edições do livro *A Fada Oriana*, de Sophia de Mello Breyner Andressen, são 972661195. Qual é o dígito de controle?

(b) Os primeiros nove dígitos do identificador ISBN-10 de uma das edições do livro *Orwell and Politics*, de George Orwell, são 014118518. Qual é o dígito de controle?