Cifra Deslocamento Simples

A cifra de Júlio César (100aC-44aC) é um cifra simples cuja chave secreta é definida pelo deslocamento que se estabelece nas letras do alfabeto (ao que se sabe esse deslocamento era de três posições).

$$e = \left(\begin{array}{cccccccccccccccccccc} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s \\ d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v \\ & t & u & v & w & x & y & z & & & & & & & & & & & \\ & w & x & y & z & a & b & c & & & & & & & & & & & \end{array} \right)$$

Mais genericamente temos

Definição (Cifra Deslocamento)

Seja $\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}^*$, $\mathcal{K} = \mathbb{Z}_{26}$. Para $0 \leq K < |\mathbb{Z}_{26}| = 26$, define-se:

$$e_K(x) = (x + K) \mod 26$$

e

$$d_K(y) = (y - K) \mod 26$$

para todo o $x, y \in \mathbb{Z}_{26}$

Congruências lineares

Uma vez que

$$\begin{cases} a \equiv c (\text{mod } m) \\ b \equiv d (\text{mod } m) \end{cases} \Rightarrow ab \equiv cd (\text{mod } m),$$

pode definir-se uma operação de multiplicação de classes de congruência em $\mathbb{Z}_m$ por:

$$[a]_m \cdot [b]_m = [ab]_m.$$

$(\mathbb{Z}_m, +, \cdot)$ é um anel comutativo com identidade. A identidade, elemento neutro da multiplicação, é $[1]_m$.

Se $m \geq 2$, $[0]_m$ não tem inverso mutiplicativo e portanto $(\mathbb{Z}_m, \cdot)$ não é um grupo.

Exemplo em $\mathbb{Z}_{14}$:

- $[5]_{14} \cdot [3]_{14} = [1]_{14}$ logo $[5]_{14}$ e $[3]_{14}$ são invertíveis e $[5]_{14}^{-1} = [3]_{14}$, $[3]_{14}^{-1} = [5]_{14}$.
- $[2]_{14}$ não é invertível, é fácil de ver que não existe um $3 \leq n \leq 13$ tal que $[2]_{14} \cdot [n]_{14} = [1]_{14}$.

Quais são os elementos invertíveis em $(\mathbb{Z}_m, \cdot)$?

Para respondera esta questão é necessário introduzir mais alguns conceitos sobre a divisibilidade em $\mathbb{Z}$.

Divisibilidades — Operações

Definição (Máximo Divisor Comum)

Dados $a, b \in \mathbb{Z}$, um inteiro não nulo c é um divisor comum de a e b se $c|a$ e $c|b$.

Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$ e considere-se $\mathcal{D} = \{c \in \mathbb{Z} : c|a \wedge c|b\}$.

$\mathcal{D} \neq \emptyset$, porque $1 \in \mathcal{D}$, e $\mathcal{D}$ é finito porque um inteiro não nulo tem um número finito de divisores.

Então $\mathcal{D}$ tem um máximo ao qual se chama **m**áximo **d**ivisor **c**omum de a e b. Esse máximo é representado por $\text{mdc}(a, b)$.

Exemplo: Os divisores comuns de 24 e 30 são $\pm 1, \pm 2, \pm 3, \pm 6$. Então $\text{mdc}(24, 30) = 6$.

Se $\text{mdc}(a, b) = 1$ diz-se que os inteiros a e b são primos entre si ou que a é primo com b.

MDC — Propriedades

Para quaisquer $a, b, c \in \mathbb{Z} \backslash \{0\}$, tem-se:

1. $\text{mdc}(a, b) = \text{mdc}(b, a) = \text{mdc}(a, -b)$;
2. $\text{mdc}\left(\frac{a}{\text{mdc}(a,b)}, \frac{b}{\text{mdc}(a,b)}\right) = 1$;
3. $\text{mdc}(a, b)$ é o menor elemento positivo de $\{ax + by : x, y \in \mathbb{Z}\}$;
4. Se $x, y \in \mathbb{Z}$ são tais que $\text{mdc}(a, b) = ax + by$ então $\text{mdc}(x, y) = 1$;
5. $\text{mdc}(a, b)$ é o único divisor comum, positivo, de a e b tal que:
$$\begin{cases} x \in \mathbb{Z} \backslash \{0\} \\ x|a \\ x|b \end{cases} \Rightarrow x | \text{mdc}(a, b)$$
6. $a|bc \wedge \text{mdc}(a, b) = 1 \Rightarrow a|c$.

Algoritmo de Euclides I

Para calcular o máximo divisor comum de $a, b \in \mathbb{Z}\backslash\{0\}$ usa-se o algoritmo de Euclides.

Teorema (Algoritmo de Euclides)

Sejam $a \in \mathbb{N}$ e $b \in \mathbb{Z}$. Aplicando sucessivamente o algoritmo da divisão obtém-se:

$$
\begin{aligned}
b &= aq_1 + r_1, \quad 0 < r_1 < a\\
a &= r_1q_2 + r_2, \quad 0 < r_2 < r_1\\
r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2\\
&\vdots\\
r_{k-2} &= r_{k-1}q_k + r_k, \quad 0 < r_k < r_{k-1}\\
r_{k-1} &= r_kq_{k+1}
\end{aligned}
$$

para um dado $k \in \mathbb{N}$ ($r_0 \coloneqq a$ e $r_{-1} \coloneqq b$).

Então $\mathrm{mdc}(a, b) = r_k$.

Algoritmo de Euclides II

Algoritmo de Euclides para o cálculo de $d = \mathrm{mdc}(a, b)$.

$\rightarrow a, b \in \mathbb{N} \wedge a \geq b$
$\leftarrow d(= \mathrm{mdc}(a, b))$.

$$
\boxed{
\begin{array}{l}
\texttt{enquanto } b \neq 0 \texttt{ faz}\\
\qquad r \coloneqq a - b\lfloor \frac{a}{b} \rfloor\\
\qquad a \coloneqq b\\
\qquad b \coloneqq r\\
\texttt{fimenquato}\\
d \coloneqq a
\end{array}
}
$$

Notas:

- $\lfloor x \rfloor$, $x \in \mathbb{R}$, denota o maior inteiro inferior ou igual a x;
- em *C++*, 'r' pode ser obtido como sendo o resto da divisão inteira de 'a' por 'b'.

Algoritmo de Euclides — Exemplo

Pode-se usar o algoritmo de Euclides para calcular $\mathrm{mdc}(2124, 396)$ e determinar $x, y \in \mathbb{Z}$ tais que: $\mathrm{mdc}(2124, 396) = 2124x + 396y$.

$$
\begin{aligned}
2124 &= 5 \times 396 + 144\\
396 &= 2 \times 144 + 108\\
144 &= 1 \times 108 + 36\\
108 &= 3 \times 36.
\end{aligned}
\qquad mdc(2124, 396) = 36
$$

Das igualdades anteriores, obtém-se

$$
\begin{aligned}
36 &= 144 - 108\\
&= 144 - (396 - 2 \times 144)\\
&= 3 \times 144 - 396\\
&= 3(2124 - 5 \times 396) - 396\\
&= 3 \times 2124 + (-16) \times 396
\end{aligned}
$$

Algoritmo de Euclides III

Algoritmo de Euclides para calcular $d = \mathrm{mdc}(a, b)$ e $x, y \in \mathbb{Z}$ tais que $d = ax + by$:

$\rightarrow a, b \in \mathbb{N}$ com $a \geq b$
$\leftarrow (d, x, y)$

$$
\boxed{
\begin{array}{l}
x_2 \coloneqq 1;\ x_1 \coloneqq 0;\ y_2 \coloneqq 0;\ y_1 \coloneqq 1;\\
\text{enquanto } b \neq 0 \text{ faz}\\
\quad q \coloneqq \lfloor \frac{a}{b} \rfloor; \qquad r \coloneqq a - qb;\\
\quad x \coloneqq x_2 - qx_1; \qquad y \coloneqq y_2 - qy_1;\\
\quad a \coloneqq b; \qquad b \coloneqq r;\\
\quad x_2 \coloneqq x_1; \qquad x_1 \coloneqq x;\\
\quad y_2 \coloneqq y_1; \qquad y_1 \coloneqq y;\\
\text{fimenquanto}\\
d \coloneqq a; x \coloneqq x_2; y \coloneqq y_2;
\end{array}
}
$$

Congruências Lineares

Se $ax \equiv b (\text{mod } m)$ com $\text{mdc}(a, m) = 1$

Proposição (Congruências Lineares)

Sejam $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ *com* $\text{mdc}(a, m) = 1$. *A congruência* $ax \equiv b (\text{mod } m)$ *tem solução e o conjunto das soluções é uma classe de congruência módulo* m.

Método de resolução de $ax \equiv b (\text{mod } m)$ com $\text{mdc}(a, m) = 1$:

Usando o algoritmo de Euclides determinam-se $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + my_0 = 1$. De $ax_0 \equiv 1 (\text{mod } m)$ resulta que $ax_0 b \equiv b (\text{mod } m)$.

O conjunto das soluções de $ax \equiv b (\text{mod } m)$ é $[x_0 b]_m$.

Caso Geral

$ax \equiv b (\text{mod } m)$

Proposição

Sejam $m \in \mathbb{N}, a, b \in \mathbb{Z}$ *e* $d = \text{mdc}(a, m)$. *A congruência* $ax \equiv b (\text{mod } m)$ *tem solução se e só se* $d | b$.

Se $d | b$ então

$$ax \equiv b (\text{mod } m) \Leftrightarrow \frac{a}{d} x \equiv \frac{b}{d} \left(\text{mod } \frac{m}{d}\right)$$

e o conjunto das soluções é a união de d classes de congruência módulo m.

Exemplo

Determinem-se as soluções de $27x \equiv 15 (\text{mod } 39)$.
$\text{mdc}(27, 39) = 3 | 15$, logo

$$27x \equiv 15 (\text{mod } 39) \Leftrightarrow 9x \equiv 5 (\text{mod } 13).$$

$\text{mdc}(9, 13) = 1$ e $1 = 3 \times 9 - 2 \times 13$. Sendo assim, $9 \times 3 \equiv 1 (\text{mod } 13)$ e $9 \times 15 \equiv 5 (\text{mod } 13)$.

O conjunto das soluções de $27x \equiv 15 (\text{mod } 39)$ é $[15]_{13} = [2]_{13} = [2]_{39} \cup [15]_{39} \cup [28]_{39}$

Inverso Multiplicativo $(\text{mod } m)$

Se $\text{mdc}(a, m) = 1$, então $[a]_m$ é invertível em $\mathbb{Z}_m$ e, sendo $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + my_0 = 1$, tem-se que:

$$[a]_m^{-1} = [x_0]_m.$$

Exemplo:
$\text{mdc}(9, 16) = 1$, logo $[9]_{16}$ é invertível em $\mathbb{Z}_{16}$: $[9]_{16}^{-1} = ?$

Resolva-se $9x \equiv 1 (\text{mod } 16)$.

$\text{mdc}(9, 16) = 1$ e $1 = 4 \times 16 - 7 \times 9$. Assim, $9 \times (-7) \equiv 1 (\text{mod } 16)$ e $[9]_{16}^{-1} = [-7]_{16} = [9]_{16}$.

Se $\text{mdc}(a, m) > 1$, $[a]_m$ não é invertível.

Os elementos invertíveis em $(\mathbb{Z}_m, \cdot)$ são os elementos de $\{[a]_m : \text{mdc}(a, m) = 1\}$.
Observação: $(\mathbb{Z}_m \backslash \{[0]_m\}, \cdot)$ é um grupo, se e só se m é primo.

Grupo Multiplicativo

Seja $U_m = \{[a]_m : \mathrm{mdc}(a, m) = 1\}$.

Teorema

Seja $m \in \mathbb{N}$. U_m é um grupo para a multiplicação de classes de congruência módulo m.

Notações:

- Quando se trabalha em $\mathbb{Z}_m$ muitas vezes representa-se $[a]_m$ apenas por r, sendo $r \in \{0, 1, \ldots, m-1\}$ o resto da divisão inteira de a por m;
- Sendo $a \in \mathbb{Z}$ e $m \in \mathbb{N}$, é usual representar por $a \bmod m$ o resto da divisão inteira de a por m;
- Se $\mathrm{mdc}(a, m) = 1$, por $a^{-1} \bmod m$ representa-se o inverso de $[a]_m$ em $\mathbb{Z}_m$.

Algoritmo de Cálculo, $a^{-1} \bmod m$

$\rightarrow a, m \in \mathbb{N}$
$\leftarrow a^{-1} \bmod m$ ou um elemento de excepção (indicando que a não é invertível módulo m).

```
m0 := m; a0 := a; t0 := 0; t := 1; q := ⌊m0/a0⌋;
r := m0 − q·a0;
enquanto r > 0 faz
        aux := t0 − q·t mod m0;
        t0 := t; t := aux;
        m0 := a0; a0 := r;
        q := ⌊m0/a0⌋; r := m0 − q·a0;
fimenquanto
Se a0 = 1 então
        devolve t;
senão
        devolve excepção;        // não tem inverso
fimse
```


Cifra de Deslocamento Linear

Definição (Cifra de Deslocamento Linear)

Seja $\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}^*$, e seja:

$$\mathcal{K} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \ : \ \mathrm{mdc}(a, 26) = 1\}.$$

Para $K = (a, b) \in \mathcal{K}$, define-se:

$$e_k(x) = (ax + b) \mod 26$$

e

$$d_k(y) = a^{-1}(y - b) \mod 26$$

para todo o $x, y \in \mathbb{Z}_{26}$

Cifras de Substituição

As cifras anteriores são casos particulares de *cifras de substituição*.
Cifras de substituição substituem símbolos (ou grupos de símbolos) por outros símbolos (ou grupos de símbolos).

Definição (Cifra de Substituição Simples)

Seja $\mathcal{A}$ um alfabeto com q símbolos e $\mathcal{M}$ o conjunto das sequências de caracteres de $\mathcal{A}$ de comprimento t. Seja $\mathcal{K}$ o conjunto de todas as permutações num conjunto $\mathcal{A}$. Define-se para cada $e \in \mathcal{K}$ uma função de encriptação como sendo:

$$E_e(m) = (E_e(m_1)E_e(m_2)\ldots E_e(m_t)) = (c_1c_2\ldots c_t) = c$$

onde $m = (m_1m_2\ldots m_t) \in \mathcal{M}$. Isto é para cada símbolo num t-tuplo, substitui-se esse símbolo por um outro símbolo de $\mathcal{A}$ de acordo com uma dada permutação e. Para decifrar $c = (c_1c_2\ldots c_t)$ calcula-se a permutação inversa $d = e^{-1}$, tendo-se então a função de desencriptação:

$$D_d(c) = (D_d(c_1)D_d(c_2)\ldots D_d(c_t)) = (m_1m_2\ldots m_t) = m$$

E_e é designada uma cifra de substituição simples, ou cifra de substituição mono-alfabética