Q1) $S=\{2,4,6,8,10,12\}$, $T=\{3,5,7,9\}$

Classifique as funções como

injetivas, sobrejetivas, bijetivas.

(a) f de S em T, f(2)=3, f(4)=3, f(6)=3, f(8)=5, f(10)=9, f(12)=7.
(b) g de T em S, g(3)=4, g(5)=8, g(7)=10, g(9)=12.
(c) h de T em T, h(3)=5, h(5)=7, h(7)=9, h(9)=9.
(d) r de T em T, r(3)=9, r(5)=5, r(7)=3, r(9)=7.
(e) p de T em T, p(3)=5, p(5)=5, p(7)=9, p(9)=9.

Q2) Seja $f(x)=x^3+3x-1$, $g(x)=x^2$.

Calcule f composto com g, f(g(x)), e

g composto com f, g(f(x)).

Q3) Determine a função inversa de

$f(x)= -4x+5$, $g(x)= 7x-10$

Criptografia Simples

Criptografia: arte de cifrar/codificar mensagens

Definir alfabeto (caracteres) a ser utilizado

A	B	C	D	E	F	G	H	I	J	K	L	M
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
13	14	15	16	17	18	19	20	21	22	23	24	25

_	!	?	,	.
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
26	27	28	29	30

Distinguir maiusculas de minusculas, incluir, se necessário, números, outros caracteres de pontuação (; : etc) e caracteres especiais ($ & # % + - = etc).

Observe que cada letra/caractere está associada a um número e nosso alfabeto (mapa de caracteres a ser utilizado) possui 31 caracteres.

Utilizamos uma função para criptografar. A função deve ser bijetiva para que se possa criptografar e descriptografar uma mensagem.

$$\text{Texto original} \quad \leftrightarrows \quad \text{Texto cifrado}$$

Função mais eficaz e simples para criptografar: $f(x) = ax+b$ com inversa $f^{-1}(x) = a'x+b'$, onde $a' = a^{-1}$ e $b' = -a^{-1}b$.

Observação: a^{-1} denota inverso multiplicativo, se $a \neq 0$ é um número, então $a \cdot a^{-1} = 1$.

Este tipo de **criptografia** é do tipo **simétrico**, de **chave de codificação secreta** (não pública). A chave de codificação são os valores a e b da função $f(x) = ax + b$ e a chave de decoficação são os valores a' e b' da função inversa de $f(x)$, $f^{-1}(x) = a'x+b'$. O motivo da chave ser não pública é que caso divulgado a e b, é muito fácil determinar a chave de decodificação $a' = a^{-1}$ e $b' = -a^{-1}b$.

Vamos utilizar congruências de números inteiros

$$a \equiv b(\text{mod } n) \Leftrightarrow a - b = q \cdot n.$$

Estamos trabalhando com um alfabeto (caracteres) que tem 31 símbolos, então iremos trabalhar com congruências módulo 31. (Caso o alfabeto tivesse 36 símbolos/caracteres, deve-se trabalhar com congruências módulo 36. De um modo geral, se trabalha com congruência módulo *quantidade de símbolos/caracteres do alfabeto*)

Como vamos trabalhar com congruências módulo 31, então a função que criptografa $f(x) = ax + b$ deve satisfazer $\text{mdc}(a, 31) = 1$.

(Caso trabalhassemos com congruências módulo 36, então a função que criptografa $f(x) = ax + b$ deveria satisfazer $\text{mdc}(a, 36) = 1$.)

Observação: mdc=máximo divisor comum.

Explicação matemática: O motivo é que $\text{mdc}(a, n) = 1 \Rightarrow$ é possível calcular o inverso multiplicativo de a, a^{-1}, na congruência módulo n.

Descobrir o inverso mulplicativo de algum número inteiro a na congruência módulo n é o mesmo que resolver um tipo de *Equação Diofantina*, a saber: determinar $p, q \in \mathbb{Z}$ que satisfazem $ap + nq = 1$ (este tipo de equação tem solução caso $\text{mdc}(a, n) = 1$).

Exemplo 1 *A função* $f(x) = 4x + 5$ *pode ser utilizada para criptografar mensagens com congruências módulo 31, porque* $mdc(4, 31) = 1$. *Vamos criptografar a mensagem* ***RUA***.

Associamos cada caractere da palavra ***RUA*** *ao seu respectivo número,*

$$R \to 17, \;\; U \to 20, \;\; A \to 0,$$

aplicamos a função $f(x) = 4x + 5$ *em cada número,*

$$f(17) = 73 \equiv 11(mod 31) \text{ e } 11 \text{ associa com a letra } L,$$

$$f(20) = 85 \equiv 23(mod 31) \text{ e } 23 \text{ associa com a letra } X,$$

$$f(0) = 5 \equiv 5(mod 31) \text{ e } 5 \text{ associa com a letra } F.$$

Logo, a mensagem original ***RUA*** *é cifrada na mensagem* LXF *através da função* $g(x) = 4x + 5$ *utilizando congruências módulo 31.*

Para descriptografar a mensagem LXF *que foi criptografada com a função* $f(x) = 4x + 5$ *utilizando congruências módulo 31, precisamos calcular* 4^{-1} *na congruência módulo 31 para determinar* $f^{-1}(x) = a'x + b'$.

$4^{-1} \equiv 8(\mod 31)$, *então* $a' = 8$ *e* $b' = 22 \Rightarrow f^{-1} = 8x + 22$.

Para decodificar a mensagem cifrada LXF, *associamos cada caractere ao seu número*

$$L \to 11,\ X \to 23,\ F \to 5,$$

e aplicamos a função inversa de $f(x)$, $f^{-1}(x) = 8x + 22$,

$$f^{-1}(11) = 110 \equiv 17(mod 31) \text{ e } 17 \text{ associa com a letra } R,$$

$$f^{-1}(23) = 206 \equiv 20(mod 31) \text{ e } 20 \text{ associa com a letra } U,$$

$$f^{-1}(5) = 62 \equiv 0(mod 31) \text{ e } 0 \text{ associa com a letra } A.$$

Portanto, obtemos a mensagem original ***RUA***.

Exemplo 2 *A mensagem* XLT!PXZV *foi criptograda com a função* $f^{-1}(x) = 8x + 22$ *em congruências módulo 31, logo é descriptograda com a função* $f(x) = 4x + 5$.