5. Usando transformações de Householder ou rotações de Givens, construa uma base ortonormada do espaço das colunas de A, com $A = \begin{bmatrix} 4 & -3 & 4 \\ 2 & -14 & -3 \\ -2 & 14 & 0 \\ 1 & -7 & 15 \end{bmatrix}$.

6. Sejam $\mathcal{X}$ e $\mathcal{Y}$ subespaços de $\mathbb{R}^3$ com bases $B_{\mathcal{X}} = \{(1,1,1),(1,2,2)\}$ e $B_{\mathcal{Y}} = \{(1,2,3)\}$.

   (a) Mostre que $\mathcal{X}$ e $\mathcal{Y}$ são complementares.

   (b) Calcule o projector P sobre $\mathcal{X}$ ao longo de $\mathcal{Y}$, assim como o seu projector complementar Q.

   (c) Determine a projecção de $v = (2,-1,1)$ sobre $\mathcal{Y}$ ao longo de $\mathcal{X}$.

Fim

⑤ No SAGE. $\longrightarrow$ Se fizermos rotações de Givens, basta fazermos a norma dos vetores, certo?

⑥ $B_X = \{(1,1,1), (1,2,2)\}$
$B_Y = \{(1,2,3)\}$

a) $u^{\perp} = \{v \in \mathbb{R}^3 : v \cdot (1,1,1) = 0 \wedge v \cdot (1,2,2) = 0\}$

$= \{v \in \mathbb{R}^3 : x + y + z = 0 \wedge x + 2y + 2z = 0\}$

$= \{v \in \mathbb{R}^3 : y = -x - z \wedge 2z = -x - 2(-x - z)\}$

$= \{v \in \mathbb{R}^3 : y = -x - z \wedge 2z = 2x + 2z\}$

$= \{v \in \mathbb{R}^3 : y = -z \wedge x = 0\}$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{bmatrix} \xrightarrow[\ell_3 \leftarrow \ell_3 - \ell_1]{\ell_2 \leftarrow \ell_2 - \ell_1} \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{bmatrix} \xrightarrow[\ell_3 \leftarrow \ell_3 - \ell_2]{} \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Após utilização do AEG, vemos que os vetores são linearmente independentes.

Temos, ainda, que $\dim \mathbb{R}^3 = 3$ e $\dim(\mathcal{X} \cup Y) = 3$.

Concluímos, desta forma, que $\mathcal{X}$ e Y são complementares.

b) P_v é a proj de v em $\mathcal{X}$ ao longo de Y

$B_{\mathcal{X}} = \{(1,1,1), (1,2,2)\}$
$B_Y = \{(1,2,3)\}$

Pela alínea anterior, $B_{\mathcal{X}} \cup B_Y = \mathbb{R}^3$

Logo $B_{3\times 3} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{bmatrix}$ é invertível.

$$PB = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 1 & 2 & 0 \end{bmatrix} = B \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\Rightarrow \quad P = B \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} B^{-1}$$

P é o projetor de v em X ao longo de Y.

Calcule-se B^{-1}:

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 2 & 0 & 1 & 0 \\ 1 & 2 & 3 & 0 & 0 & 1 \end{array}\right] \xrightarrow[\substack{l_2 \leftarrow l_2 - l_1 \\ l_3 \leftarrow l_3 - l_1}]{} \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 1 & 0 \\ 0 & 1 & 2 & -1 & 0 & 1 \end{array}\right] \xrightarrow[\substack{l_1 \leftarrow l_1 - l_2 \\ l_3 \leftarrow l_3 - l_2}]{} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & -1 & 0 \\ 0 & 1 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 \end{array}\right]$$

$$\xrightarrow[l_2 \leftarrow l_2 - l_3]{} \left[\begin{array}{ccc|c} 1 & 0 & 0 & \\ 0 & 1 & 0 & \underbrace{\begin{matrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{matrix}}_{B^{-1}} \\ 0 & 0 & 1 & \end{array}\right]$$

$$P = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 1 & 2 & 0 \end{bmatrix} \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{bmatrix}$$

$-1+2$

$-1+4$

$$= \begin{bmatrix} 1 & 1 & -1 \\ 0 & 3 & -2 \\ 0 & 3 & -2 \end{bmatrix}$$

proj complementar i.e. proj em Y ao longo de X.

$$Q = I - P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 1 & -1 \\ 0 & 3 & -2 \\ 0 & 3 & -2 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 1 \\ 0 & -2 & 2 \\ 0 & -3 & 3 \end{bmatrix}$$

c) $$Qv = \underbrace{\begin{bmatrix} 0 & -1 & 1 \\ 0 & -2 & 2 \\ 0 & -3 & 3 \end{bmatrix}}_{3\times 3} \underbrace{\begin{bmatrix} 2 \\ -1 \\ 1 \end{bmatrix}}_{3\times 1} = \begin{bmatrix} 2 \\ 4 \\ 6 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$$

comprimento da projeção.

1. Considere a curva elíptica E definida por $y^2 = x^3 + 3084x + 109841$ sobre $\mathbb{Z}_{191123}$ e $P = ((123483 : 23340 : 1)) \in E$. Considere a chave pública Elgamal (E, P, Q) com $Q = rP = (130256 : 107534 : 1)$, para algum r. Cifre a mensagem **mens=112** (não se esqueça que em primeiro lugar tem que converter **mens** num ponto da curva elíptica E).

→ confirmar c/ prof se a mensagem cifrada é (γ, δ) com $\gamma = k \cdot P$
$\delta = k \cdot Q + \text{mens}.$

ou

(γ, δ) com $\gamma = k\, Q + \text{mens}$
$\delta = k \cdot P.$

2. Considere o primo $p = 874537$. Defina uma curva elíptica E sobre os inteiros módulo p. Usando parâmetros à sua escolha, use o sistema Menezes-Vanstone para cifrar **mens=(501, 1112)** na curva elíptica E. Conhecendo a chave privada, decifre o que cifrou.

O que é que podemos levar para o teste?

3. Factorize, usando o método de Lenstra, o número $n = 28321$, usando a curva elíptica $E : y^2 = x^3 + 17622x + 10185$ sobre $\mathbb{Z}_n$, e $P = (18640 : 5420 : 1) \in E$, tomando o parâmetro $B = 100$.

O código não corre. → qualquer coisa com $P \times$ Pari.

ou

E. field.

4. Seja $n \geq 3$ um natural ímpar com k factores primos $p_1, \ldots, p_k$ distintos e tal que $n = \prod_i p_i$. Mostre que existem, módulo n, exactamente 2^k raizes quadradas de 1.

Seja $n \in \mathbb{N}$ tal que $n \geq 3$ e cuja fatorização em k primos distintos é dada por $n = \prod_{i=1}^{k} p_i$.

Queremos mostrar que $\underbrace{\text{existem exatamente } 2^k \text{ raízes quadradas de } 1 \text{ módulo } n.}_{P(k)}$

Pelo PIM, basta mostrar

- $P(1)$
- Se $P(k)$, então $P(k+1)$.

$\boxed{\text{Passo de base}}$

Temos $k = 1$

$P(1)$ se existem 2^1 raízes quadradas de 1 módulo p

Ora,
- $1^2 \equiv 1 \pmod p$, logo 1 é res. quadrático de 1 mod p

$$\begin{aligned} \cdot (p-1)^2 &\equiv p^2 - 2p + 1 \mod p \\ &\equiv 0 + 0 + 1 \mod p \\ &\equiv 1 \mod p, \end{aligned}$$

logo $p-1$ é resíduo quadrático de 1 módulo p.

1 mod 3

mod 3.

$\boxed{\text{Passo de indução}}$

Suponhamos $P(k)$, i.e., para um certo $n = p_1 \ldots p_k$, existem 2^k raízes quadradas de 1 modulo n.

Queremos mostrar $P(k+1)$, i.e., para um certo $m = p_1 \ldots p_k p_{k+1}$, existem 2^k raízes quadradas de 1 módulo m.

Ora, resolver $x^2 \equiv 1 \mod m \iff \begin{cases} x^2 \equiv 1 \mod p_1 \\ x^2 \equiv 1 \mod p_2 \\ \vdots \\ x^2 \equiv 1 \mod p_k \\ x^2 \equiv 1 \mod p_{k+1} \end{cases}$

Para cada uma das congruências temos 2 soluções $x \equiv \pm 1 \mod p_i$, $i \in \{1, \ldots, k+1\}$.

Pelo Teorema Chinês dos Restos, o sistema de congruências tem uma solução única módulo m.

A sequência

$$\frac{p-1}{2(p+1)} + \frac{2}{p+2} = \frac{3p+1}{2p+2}$$