Tutorial 8b

Test 2 (Questions and Solutions)

Question 1: Orthogonal Vectors

- The two vectors, $(-2, 0, 1)$ and $(3, 3, a)$, are orthogonal. Find the value of a.

- Solution:
  - For orthogonal vectors, their inner product is equal to zero:

$$(-2)(3) + (0)(3) + (1)(a) = 0$$

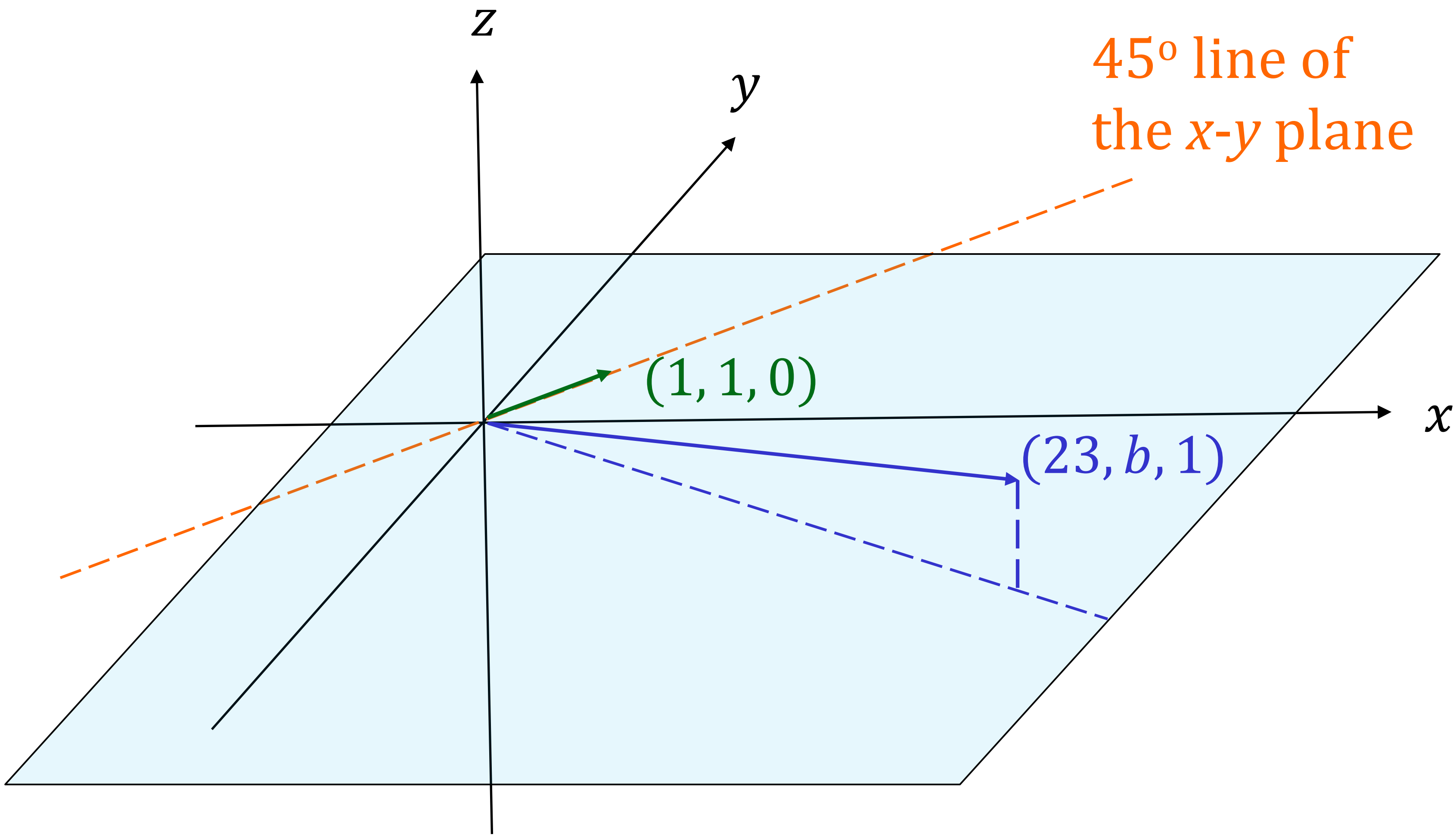
  - Therefore, $a = 6$.

Question 2: RMS error

- We have four data values, 13, 16, 17, and x, and the best estimate that minimizes the RMS error is 10. What is the RMS error of this estimate? Round your answer to two decimal places.
- Solution:
  - The best estimate that minimizes the RMS error is just the average of the data values.
  - Therefore, $(13 + 16 + 17 + x)/4 = 10 \implies x = -6$.
  - RMS error = $\sqrt{\frac{(13-10)^2+(16-10)^2+(17-10)^2+(-6-10)^2}{4}} = 9.35$

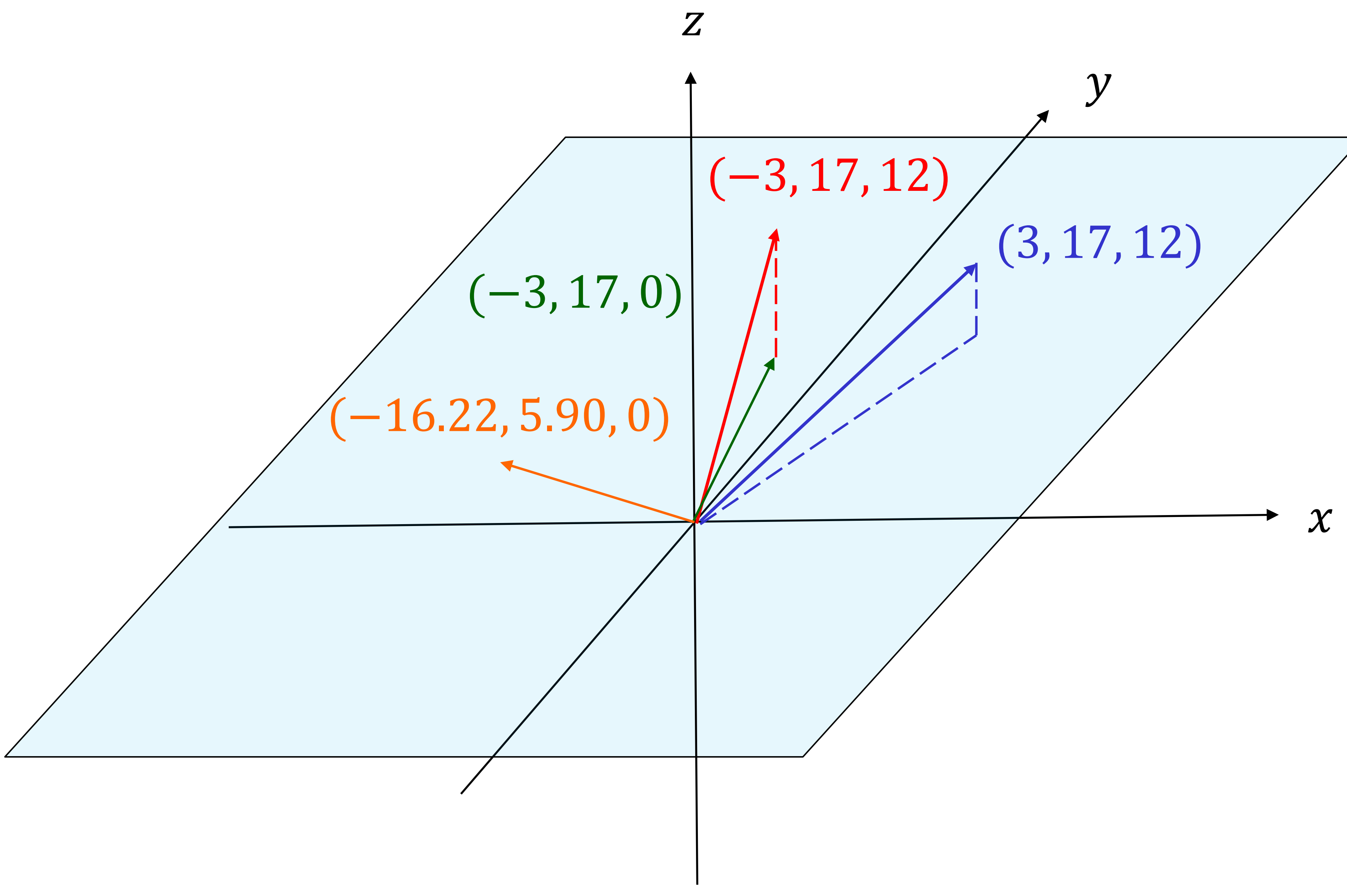
Question 3: Projection

- The vector $(23, b, 1)$ is projected onto the 45^o line of the *x*-*y* plane. Given that the length of the vector after projection is 5, find the value of b. Round your answer to 2 decimal places.
- Solution:
  - A vector that represents the 45^o line or the x-y plane is $(1, 1, 0)$.
  - Projection onto that line is given by the inner product between $(23, b, 1)$ and $(1, 1, 0)$, and the division by the norm of $(1, 1, 0)$. Therefore, the length of the vector after projection is $\frac{23+b}{\sqrt{2}}$.
  - Hence, $\frac{23+b}{\sqrt{2}} = 5$ implies $b = -15.93$.


z
y
45o line of
the x-y plane
$(1, 1, 0)$
x
$(23, b, 1)$

Question 4: Geometric Transformations

- Consider the vector $(3, 17, 12)$. First, it is reflected across the *y*-*z* plane. Next, it is projected onto the *x*-*y* plane. Lastly, it is rotated anti-clockwise by 60^o on the *x*-*y* plane. What is the *x*-component of the resultant vector? Round your answer to 2 decimal places.
- Solution:
  - Reflection across the *y*-*z* plane: $(-3, 17, 12)$.
  - Projection onto the *x*-*y* plane: $(-3, 17, 0)$.
  - Rotation anti-clockwise by 60^o on the *x*-*y* plane:
$$\begin{bmatrix} \cos 60^o & -\sin 60^o \\ \sin 60^o & \cos 60^o \end{bmatrix} \begin{bmatrix} -3 \\ 17 \end{bmatrix} = \begin{bmatrix} -16.22 \\ 5.90 \end{bmatrix}.$$
  - Hence, the *x*-component is -16.22.



z
y
x
$(-3, 17, 12)$
$(3, 17, 12)$
$(-3, 17, 0)$
$(-16.22, 5.90, 0)$

Question 5: Cryptography

- Bob wants to encrypt a non-negative number x, where x is smaller than 65. First , he applies a linear cipher to produce $y = 11x + 13 \pmod{65}$. Next, he applies the RSA encryption method with the public keys $N = 65$ and $e = 29$. Given that the ciphertext is 8, find the value of x.

Question 5 (Solution)

(RSA)

- $N = 65$ implies $p = 13, q = 5$.
- $\emptyset(N) = (p - 1)(q - 1) = (12)(4) = 48$
- $29d \equiv 1 \pmod{48}$
- $d \equiv 5 \pmod{48}$
- $y \equiv 8^5 \equiv 8 \pmod{65}$

You can use SageMath or Extended Euclidean Algorithm to find $29^{-1} \pmod{48}$.

(Linear/Affine Cipher)

- $x \equiv 11^{-1}(y - 13) \pmod{65}$

$$\equiv 6\,(8 - 13)$$

$$\equiv 35 \pmod{65}$$

It can be directly observed that

$$11^{-1} \equiv 6 \pmod{65},$$

since

$$11 \times 6 \equiv 66 \equiv 1 \pmod{65}$$

Question 6: Subspace

- Consider the three-dimensional vector space $\mathbb{R}^3$. Let S be its subset which consists of all linear combinations of $(1, -1, 2)$ and $(1, 2, 3)$. Prove or disprove that S is a subspace of $\mathbb{R}^3$.
- Proof:
  - $S = \{\alpha(1, -1, 2) + \beta(1, 2, 3)\}$.
  - Pick two arbitrary vectors from S.
    - $v_1 = \alpha_1(1, -1, 2) + \beta_1(1, 2, 3)$
    - $v_2 = \alpha_2(1, -1, 2) + \beta_2(1, 2, 3)$
  - Closed under addition:
    - $v_1 + v_2 = (\alpha_1 + \alpha_2)(1, -1, 2) + (\beta_1 + \beta_2)(1, 2, 3) \in S$
  - Closed under scalar multiplication:
    - $cv_1 = c\alpha_1(1, -1, 2) + c\beta_1(1, 2, 3) \in S$
  - Hence, S is a subspace of $\mathbb{R}^3$.

Proof Method:
1. Pick two arbitrary elements from the set.
2. Check the two conditions:
   - ✓ Closed under additions.
   - ✓ Closed under scalar multiplication.

Q.E.D.

Question 7: Simultaneous Congruences

- (a) Use the extended Euclidean algorithm to find $\gcd(109, 97)$ and a solution in integers to the equation $109x + 97y = \gcd(109, 97)$.
- Solution:

$\gcd(109, 97)$=1
$x = -8, y = 9$

109	**97**		
1	0	109	a
0	1	97	b
1	-1	12	c=a-b
-8	9	1	d=b-8c

Note: You can find any solution that satisfies $x = -8 + 97t, y = 9 + 109t, t \in \mathbb{Z}$.

Question 7: Simultaneous Congruences

- (b) Hence, find the smallest positive value of z that solves the following simultaneous congruences:

$$z \equiv a \pmod{109}, \qquad z \equiv b \pmod{97}$$

- Solution:

From lecture notes of Unit 6 (Page 6-15), we can find

$$z = (a)(97)(9)+(b)(109)(-8) \pmod{10573}$$

For example, if $a = 1, b = 23$, then

$$z = -19183 \pmod{10573} = 1963$$