Q1 [5 points] Consider the quantum money protocol that we learnt and answer the below questions from the point of view of a malicious person who is traditionally named Eve. Eve receives a note from a legitimate channel, say with denomination D, serial number S, and qubit in state $|\psi\rangle$; she prepares a forged note in the following manner.

She randomly decides between two measurement X or Z and measures $|\psi\rangle$ using that measurement. Suppose the outcome is $|\psi'\rangle$. She creates a qubit in the state $|\psi'\rangle$ for her duplicate note. She uses creates a fake note using $|\psi'\rangle$ with denomination D and serial number S.

Then, to legitimise her note, she presents the note to the bank for verification. This exercise will help you compute Eve probability of success.

1. Suppose $|\psi\rangle = |0\rangle$. What is the probability that $|\psi'\rangle = |\psi\rangle$? $\frac{1}{2}.1 + \frac{1}{2}.0 = \frac{1}{2}$.
2. Prove that the bank always successfully verifies the note if $|\psi'\rangle = |\psi\rangle$. State in the note matches with what bank has on record.
3. What is the probability that the bank successfully verifies the note if $|\psi'\rangle \neq |\psi\rangle$ when $|\psi\rangle = |0\rangle$? $|\psi'\rangle$ can be $+$ or $-$ with probability $1/2$ each; in each case, bank verification is successful with probability $1/2$. Total prob. $= 1/2$.
4. Prove that the bank successfully verifies the note with only $\frac{1}{2}$ probability if $|\psi'\rangle \neq |\psi\rangle$ for all possible $|\psi\rangle$. Similar to 3, prob. $= 1/2$.
5. Now combine both the cases of $|\psi'\rangle = |\psi\rangle$ and $|\psi'\rangle \neq |\psi\rangle$ to compute the probability of the bank successfully verifying the note. $\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot 1 = \frac{3}{4}$.

Q2 [3 points] Write down the action of $\sqrt{X}$, $\sqrt{Y}$, $\sqrt{Z}$ gates in any one of these basis: standard basis, Hadamard basis, $\{|+i\rangle, |-i\rangle\}$ (we will refer to this as the CP-basis – CP stands for circular polarization).

$$\sqrt{Z} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \sqrt{X} = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} e^{\iota\pi/4} & e^{-\iota\pi/4} \\ e^{-\iota\pi/4} & e^{\iota\pi/4} \end{bmatrix}, \sqrt{Y} = \frac{1}{2}\begin{bmatrix} 1+i & -1-i \\ 1+i & 1+i \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} e^{\iota\pi/4} & -e^{\iota\pi/4} \\ e^{-\iota\pi/4} & e^{\iota\pi/4} \end{bmatrix}$$

The actions of $\sqrt{X}$ and $\sqrt{Y}$ can be expressed better in their respective eigenstates.

$$X = 1 \cdot |+\rangle\langle+| + (-1) \cdot |-\rangle\langle-| \, , \sqrt{X} = 1 \cdot |+\rangle\langle+| + \iota \cdot |-\rangle\langle-|$$

$$Y = 1 \cdot |+i\rangle\langle+i| + (-1) \cdot |-i\rangle\langle-i| \, , \sqrt{Y} = 1 \cdot |+i\rangle\langle+i| + \iota \cdot |-i\rangle\langle-i|$$

Q3 [3 points] Recall that X acts like a NOT-operator in the standard basis. Show that Z, Y and H too act like a NOT-operator in some basis. Write down the states of all the three bases in either the standard basis, the Hadamard basis, or the i basis.

Z acts as NOT in the Hadamard basis, Y acts as NOT in the $\{|0\rangle, \iota|1\rangle\}$ basis and in the $\{|+\rangle, -i|-\rangle\}$. H acts as NOT in the basis $\{e^{i\pi/4}|+i\rangle, e^{-i\pi/4}|-i\rangle\}$.
There is an intuitive approach, using the Bloch sphere, to perform the same task for any arbitrary operator. Eigenvectors of H are: $\frac{1\pm\sqrt{2}}{\sqrt{4\pm2\sqrt{2}}}|0\rangle + \frac{1}{\sqrt{4\pm2\sqrt{2}}}|1\rangle$ with eigenvalues ±1. The Bloch vector (θ, ϕ) corresponding to eigenvalue 1 is the axis of rotation for H; that corresponds to $\cos\frac{\theta}{2} = \frac{1+\sqrt{2}}{\sqrt{4+2\sqrt{2}}}$, $e^{\iota\phi}\sin\frac{\theta}{2} = \frac{1}{\sqrt{4+2\sqrt{2}}}$, from which we get $\cos\theta = \pi/4$ and $\phi = 0$. Thus, H is a rotation about the Bloch vector $(1, 0, -1)/\sqrt{2} = (X + Z)/\sqrt{2} \equiv (\pi/4, 0)$.
This implies that H is a reflection about the plane perpendicular to $(1, 0, 1)/\sqrt{2}$ and any two vectors in that plane that form a basis can be the basis we are looking for.
One such vector is $(1, 0, -1)/\sqrt{2} \equiv (3\pi/4, 0)$; Since basis vectors lie diametrically opposite in the Bloch sphere, the other vector (still perpendicular to the axis) must be $(-1, 0, 1)/\sqrt{2} \equiv (\pi/4, \pi)$. Represented in the standard basis, the corresponding states are:

$$\cos(3\pi/8)|0\rangle + \sin(3\pi/8)|1\rangle, \cos(\pi/8)|0\rangle + e^{i\pi}\sin(\pi/8)|1\rangle$$

Another pair is $(0, 1, 0) \equiv (\pi/2, \pi/2)$ and $(0, -1, 0) \equiv (\pi/2, 3\pi/2)$; these correspond to the $|+i\rangle$ and $|-i\rangle$ states.

Q4(a) [0 points, do not submit] Read about 3D rotations using Euler angles.

Q4(b) [0 points, do not submit] Understand how $R_Z(\theta)$ and $R_Y(\theta)$ modifies the above basis states for different values of θ.

Q5 [1+3+4+3+1+2=14 points] In this question you will design and implement the following operator:

$$U = |+i\rangle\langle 0| + |-i\rangle\langle 1|$$

1. Write down the matrix form of U. $U = \frac{1}{\sqrt{2}}[1, 1; i, -i]$.

2. Apply U on the states in the standard basis, states in the Hadamard basis, and states in the CP-basis. You should write the output states in the standard basis.

$$|0\rangle \to |+i\rangle\,, \qquad |1\rangle \to |-i\rangle$$
$$|+\rangle \to |0\rangle\,, \qquad |-\rangle \to \iota\,|1\rangle$$
$$|+i\rangle \to \tfrac{1+i}{2}\,|0\rangle + \tfrac{1+i}{2}\,|1\rangle = \tfrac{1+i}{\sqrt{2}}\,|+\rangle\,, \qquad |-i\rangle \to \tfrac{1-i}{2}\,|0\rangle - \tfrac{1-i}{2}\,|1\rangle = \tfrac{1-i}{\sqrt{2}}\,|-\rangle$$

3. Draw a Bloch sphere and show these states on the sphere: $U\,|0\rangle$, $U\,|1\rangle$, $U\,|+\rangle$, $U\,|-\rangle$.

4. Any 3D rotation can be decomposed as three rotations: about Z by γ, about Y by δ, about Z by β. With the help of trial-and-error, identify β, δ, γ such that the sequence performs the same mapping as U on $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$. The angles should also satisfy $U = e^{\iota\alpha} R_Z(\beta) R_Y(\delta) R_Z(\gamma)$ for some α. *Hint: Use 3D rotation ideas. The angles are either $0, \pi/2$ or π, so there are only a few combinations.* $U = e^{i\cdot 5\pi/4} R_Z(\pi/2) R_Y(\pi/2) R_Z(\pi)$).

5. Use Qiskit composer to create a 1-qubit circuit that first applies $R_Z(\gamma)$, then applies $R_Y(\delta)$, and finally $R_Z(\beta)$. Add a measurement to a classical register.

```
circuit.rz(np.pi, qreg_q[0])
circuit.ry(np.pi / 2, qreg_q[0])
circuit.rz(np.pi / 2, qreg_q[0])
circuit.measure(qreg_q[0], creg_c[0])
```

6. Copy the python code that created the circuit. Then paste it inside this boiler-plate code. You can either install qiskit on your computer or use Google colab for the same.

```
from qiskit import QuantumCircuit, transpile, QuantumRegister, ClassicalRegister
from qiskit_aer import AerSimulator
from qiskit_aer.noise import NoiseModel, pauli_error, depolarizing_error
from qiskit.providers.basic_provider import BasicSimulator
import numpy as np
import math

# add your circuit here
# make sure the object for QuantumCircuit is named 'circuit'

backend = BasicSimulator()

# Run the circuit on |0> and get the results
job = backend.run(circuit, shots=1000, initial_statevector = np.array([1, 0]))
result = job.result()
counts = result.get_counts()

print(counts)
```

Print the `counts` that the code outputs for different `initial_statevector` corresponding to $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$. Both outcomes are equally likely for the initial states $|0\rangle$ and $|1\rangle$. When the initial state is $|+\rangle$, only 0 is observed, and when the initial state is $|-\rangle$, only 1 is observed.