Question 1

[3]

Prove that $111^{333} + 333^{111}$ is divisible by 7.

Question 2

[3]

Let us consider RSA cryptosystem with $N = 25591$ and $\phi(N) = 25272$. Find p and q where $N = p \times q$. Describe your efficient algorithm. Note that the school book factorization algorithm is a trivial and inefficient algorithm.

Question 3

[1+1+2]

Suppose $D = \begin{pmatrix} \frac{1}{2} + \frac{1}{2}i & -\frac{1}{2} - \frac{1}{2}i \\ \frac{1}{2} + \frac{1}{2}i & \frac{1}{2} + \frac{1}{2}i \end{pmatrix}$. Compute $D|0>, D|1> \textit{and } D^2$.

Question 4

[2]

For an elliptic curve, which of the following statements are true? There can be more than one correct answer:

1. The points on the elliptic curves form an additive group.
2. Consider two points,P and Q with the relationship $P = [k]Q$, where k is a scalar. It is easy to compute k from the knowledge of P and Q.
3. Scalar multiplication operation on an elliptic curve can be computed without doing any point addition
4. The point of infinity O is the additive identity for the points on the elliptic curve

Question 5

[3]

Consider the following affine addition formula of two points $P(x_1, y_1)$ and $Q(x_2, y_2)$. The result of the addition is $R(x_3, y_3)$. Convert this affine addition formula into projective coordinate addition formula.

$$x_3 = \frac{x_1.y_2}{x_2.y_1}$$

$$y_3 = \frac{x_1 + x_2.y_2}{x_1.y_2}$$

Question 6

[3]

Fill in the blanks: In 4 way handshake of WPA2, first two messages are exchanged between the Supplicant and the Authentication to share _____ , _____ and _____.

Question 7

[3]

If the message m is changed to $m^{'}$ in the verification phase of the pederson commitment, how will the protocol react at the verifier end? Explain with control flow of the protocol.

Question 8

[4]

What would be the circuit output of Figure 1? Also, state what quantum feature this circuit exhibits.

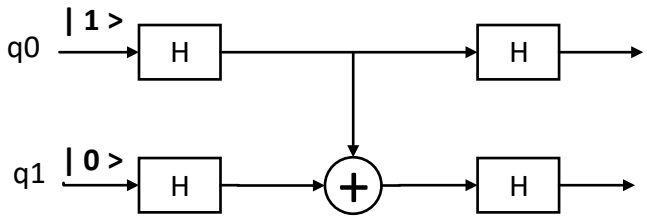

Figure 1: Target Quantum Circuit for Question no: 9