Assignment week 7

1. When calculating the sensitivity in ε-Differential Privacy where the values to be derived from the data points is a d-dimension vector, identify the normalisation technique. (Notations are the same as used in the lecture)
    a. Manhattan normalisation
    b. Eucledian normalisation
    c. Max normalisation
    d. Min-max normalisation
    e. Sigmoid normalisation

2. In (ε, δ)- Differential privacy what does δ=0 imply? (Notations are the same as used in the lecture)
    a. The equation $(P(M(x) \epsilon S) \leq e^{\varepsilon} (P(M(x') \epsilon S)$ should hold for some of the subsets S
    b. The equation $(P(M(x) \epsilon S) \leq e^{\varepsilon} (P(M(x') \epsilon S)$ should hold for most of the subsets S
    c. The equation $(P(M(x) \epsilon S) \leq e^{\varepsilon} (P(M(x') \epsilon S)$ should hold for all of the subsets S
    d. The equation $(P(M(x) \epsilon S) \leq e^{\varepsilon} (P(M(x') \epsilon S)$ should hold for none of the subsets S

3. How do the utilities vary in the Laplacian mechanism vs the Gaussian mechanism in a higher dimension differential privacy setting?
    a. As the dimension increases, the Gaussian mechanism requires quadratically more amount of noise than the Laplacian mechanism, decreasing the utility
    b. As the dimension increases, the Gaussian mechanism requires quadratically lesser amount of noise than the Laplacian mechanism, decreasing the utility
    c. As the dimension increases, the Gaussian mechanism requires quadratically lesser amount of noise than the Laplacian mechanism, increasing the utility
    d. As the dimension increases, the Gaussian mechanism requires quadratically more amount of noise than the Laplacian mechanism, increasing the utility

4. ______ property ensures that a function applied on the privacy-protected data ______ its privacy aspect after applying a function over it.
    a. i. Post-processing ii. Retains
    b. i. Post-processing ii. Loses
    c. i. Composition ii. Retains
    d. i. Composition ii. Loses

5. After using **k** mechanisms for getting **k** (ε, δ)- differentially private data variations for a dataset, the combined leakage that is observed from these **k** mechanisms can be minimized by:
    a. Using Laplacian Mechanism
    b. Using Gaussian Mechanism
    c. Using Uniform Mechanism
    d. Using Exponential Mechanism

6. In a buyer-seller problem, given **n** buyers and **n** valuations by the buyers, what is the total **revenue** given a price **p**.
    a. $p \sum_{i=n}^{n} A \;\; where\ A = 1\ if\ v_i \geq p\ and\ \ A = 0\ \ if\ v_i \leq p$
    b. $p \sum_{i=n}^{n} A \;\; where\ A = 0\ if\ v_i \geq p\ and\ \ A = 1\ \ if\ v_i \leq p$
    c. pn
    d. $p(n - 1)$
    e. $p(1/n)$

7. In the exponential mechanism to calculate the price to maximize the revenue, identify the correct statement in the scenario where 2 unequal prices result in the same revenue:
    a. Both prices have an unequal probability of being selected
    b. Both prices have an equal probability of being selected
    c. A higher price has a higher probability of being chosen due to normalisation
    d. A lower price has a higher probability of being chosen due to normalisation

8. In a classification problem, if a data point lies on a hyperplane that perfectly separates the two classes, the probability of the data point belonging to class A is:
    a. 25%
    b. 50%
    c. 75%
    d. 100 %

9. In a vanilla Principle Component Analysis method, the reconstruction loss of a protected group is ________ than the remaining data before resampling and ________ than the remaining data after resampling.
    a. Higher, higher
    b. Higher, lower
    c. Lower, higher
    d. Lower, lower

10. The goal of a Fair PCA is to find a PCA solution U where U=[Ua, Ub] such that reconstruction loss of the two groups A and B where A is the protected group is:
    a. Equal
    b. Unequal
    c. The protected group has a lower reconstruction loss
    d. The protected group has a higher reconstruction loss

11. In an ideal situation where the models are completely fair, the different parity values are:
    a. Approach 0
    b. 1
    c. Approach 1
    d. 0

12. Match the following:

    i. $P(M(x) = 1 \mid x \; in \; C) - P(M(x) = 1)$ — a. Fair Logistic regression

    ii. $P(M(x) = 1 \mid y = 1 \; and \; C) - P(M(x) = 1 \mid y = 1)$ — b. Statistical Parity

    iii. $P(M(x) = 1 \mid C = 1) - P(M(x) = 1 \mid C = 0)$ — c. Equality of Opportunity

    a. i. - a, ii. - b, iii. - c
    b. i. - b, ii. - a, iii. - c
    c. i. - c, ii. - a, iii. - b
    d. i. - b, ii. - c, iii. - a