ENEE 457
Differential Privacy Class Exercise

1. Show that mechanism M defined below is not differentially private, using the definition of differential privacy and the databases D and D’ defined below.

   M randomly chooses a set of 3 records and returns the number of UMD students in the randomly chosen set.

Name	UMD Student
Alice	0
Bob	0
Charlie	0
Daniel	1
Edgar	0

Name	UMD Student
Alice	0
Bob	0
Charlie	0
Edgar	0

Solution. The range $R(M)$ is non-negative integers. Let $S \subseteq R(M)$ be $S = \{1\}$. Then we have

$$\Pr[M(D) \in S] = \frac{3}{5}, \Pr[M(D') \in S] = 0.$$

This contradicts differential privacy.