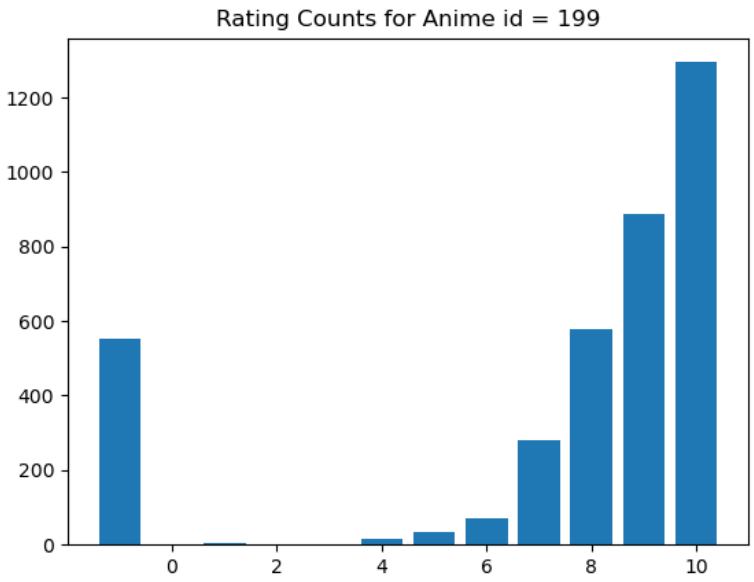
Part 2 DP Implementation



This histogram represents the users true values.

Laplace Mechanism

AVERAGE ERROR

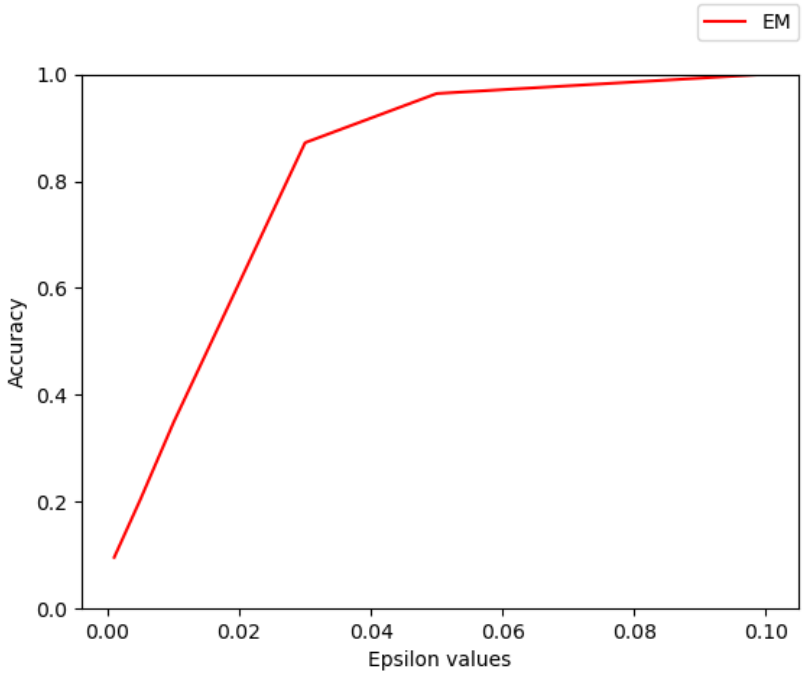
Epsilon	Error
0.0001	18865.058884798997
0.001	1922.8952293662346
0.005	391.45673324340316
0.01	205.0631030114444
0.05	39.26135657153531
0.1	21.061126252439692
1	2.1357372821512426

MEAN SQUARED ERROR

Epsilon	Error
0.0001	703337576.7415311
0.001	7151508.1651207255
0.005	289422.4377802933
0.01	83641.75225226901
0.05	2856.899051607393
0.1	875.1742792062929
1	8.928583287313447

The first table shows the Average Error of corresponding epsilon value, and the second table shows the Mean Squared Error of the corresponding epsilon value. I re-run the experiment for each epsilon 40 times and gets the average of the errors. As we can see, when we increase the epsilon value the errors get lower. The reason is privacy is getting low when we increase the epsilon.

Exponential Mechanism



This graph shows the Accuracy of the Exponential Mechanism. I re-run the experiment for each epsilon 1000 times and get the average of that results accuracy. When we increase the epsilon values the accuracy of EM is getting higher. The reason is privacy is getting low when we increase the epsilon. That's why we can easily guess the most rated anime from the dataset. I did not expect the accuracy rate to reach 100 percent in such a low epsilon. performance of this accuracy rate is also dependent on the dataset. If we had worked with data whose results were closer to each other (meaning the score functions), we would not have been able to reach 100 percent of such a low epsilon value