

CS 355, Fall, 2019, Homework 1

1. In a dictionary used for solving substitution ciphers, there are 10578 seven-letter words. Of these, 644 have first letter A and 766 have last letter Y. Fifty words (like ABILITY and ARCHERY) have both first letter A and last letter Y. You are trying to guess the plaintext word for a seven-letter ciphertext word. Assume the plaintext word is in the dictionary. Assume that all words in the dictionary are equally likely to be the one you are trying to guess.

Write your answers as fractions like $87/218$.

- a. What is the probability that the first letter of the plaintext word is A?
- b. What is the probability that the last letter of the plaintext word is Y?
- c. What is the probability that the last letter of the plaintext word is Y given that the first letter is A?
- d. Use Bayes' Theorem to find the probability that the first letter of the plaintext word is A given that the last letter is Y. Check your answer by computing this probability directly.

2. a. Show all your work as you find the greatest common divisor of 8239 and 12551.

b. Show all your work as you use the extended Euclidean algorithm to find integers x and y so that $8239x + 12551y = \gcd(8239, 12551)$.

3. Approximately (within 10%, say) how many prime numbers are there between e^{400} and $e^{400} + 8 \cdot 10^{10}$? Give a cogent reason for your answer. Do not write a program to try to count these primes.