

A. I wish to use the Miller-Rabin probabilistic primality test to determine whether or not $n = 121$ is prime. There are $n - 3 = 118$ possible bases $a \in \{2, \dots, n - 2\}$. For how many of these bases a does n pass the test, even though it is not prime? Give an exact answer (perhaps by writing a short program).

B. As we've discussed in class, I wish to send the message 0110 to my friend using one parity bit of error correction. (The actual message is 011; the last 0 is the parity bit.) Suppose that each of the four bits has a 1% chance of incurring an error during transmission. Assume that the errors on the four bits are mutually independent (see page 458). Given that my friend receives a message of even parity, what is the probability that it is the correct message (that is, no errors have occurred)?

Also complete Problems 8, 11, 19, 21 in Section 7.3.